Mult-IP™ Mobile VPN
Administration Guide
Version 3.11.2

By Radio IP Software

CERTIFIED SECURED BY RSA PARTNER

Document Description

Mult-IP Mobile VPN 3.11 Administration Guide
Doc num.:106-0000001128-0140

Written and published by: Radio IP Software, Inc. - 1111 St. Charles St. W. – East Tower - Suite 555 - Longueuil, Quebec J4K 5G4 - North American
Toll Free: +1 877-717-2242 - Telephone: +1 514-890-6070 - Fax: +1 514-890-1332 - Website: www.radio-ip.com
For Technical Support: support@radio-ip.com

Table of Contents

Welcome to Mult-IP 3.11.2

This document map is provided to help you navigate through this end-user documentation. Click to jump to the topic area that interests you the most:

Introducing Mult-IP Mobile VPN

Thank you for choosing Radio IP as your mobile VPN solution. The *Mult-IP Administration Guide* contains all the information you need to configure Mult-IP assets and manage mobile fleet traffic. This documentation is available in the following formats:

- **Online** - Click the **Mult-IP Help** (?) button in the management console's **Actions** pane (rightmost area) or context menus to access the searchable, topic-based version of this administration guide;
- **PDF** - A printable PDF (PDF) file can be found in the *Documentation* folder of your Mult-IP CD or zip archive (requires Adobe® Acrobat Reader or browser plug-in for viewing).

Mult-IP documentation is subject to frequent revisions in order to keep pace with this rapidly evolving product. While updated documentation always accompanies new software releases, we do welcome your feedback on any omission or inconsistency encountered between the documentation and actual software or GUI behavior.

Mult-IP system overview

Radio IP's flagship secure mobile VPN solution extends the reach of your corporate LAN over concurrent private and public wireless networks. The ability to maintain a connection using several simultaneous radio links allows a mobile workforce to maintain efficient field office by accessing specific applications and online resources with a level of security that rivals that of the corporate LAN.

Mult-IP employs gateways to route packets to and from mobile devices, LAN servers (application, authentication and mail) and the Internet over a virtual segment isolated from the corporate LAN. To support concurrent networking, resilience to traffic peaks while handling a large fleet spread across multiple agencies, Mult-IP applies load-balancing which dynamically distributes traffic across multiple gateways.

Client traffic packets are either accepted or dropped when reaching the gateways following customer-defined rules based on destination IPs and ports. Accepted packets are routed to pipes individually configured to distinguish between broadband and narrowband traffic, with each pipe using concurrent communication drivers to optimize wireless performance and ensure connection and session persistence in the event of an out-of-coverage condition forcing roaming to another network. To this end, Mult-IP supports an expanding range of wireless data communication drivers: from public broadband carriers, wireless ISPs (WI-FI or WiMax) and satellite to Professional Mobile Radio (PMR) systems used in their most efficient form through Radio IP's streamlined TCP-IP algorithm.

The system uses an MMC-type management console for overall system configuration and fleet provisioning through group policies and remote client software updates. Functional nodes are used to emulate the organizational structure. They are logically arranged in a top-down structure and support the definition of as many custom groups as are needed to meet logical fleet distribution through all corporate agencies.

System Highlights

Below are some benefits and innovative technologies put forward in the Mult-IP Mobile VPN solution:

- **Network Agnostic** - Mult-IP supports all wireless networks, from PMR (IP or non-IP based), public/private wireless (cellular, Wi-Fi, LTE, WiMAX) to satellite networks.
- **Network Optimization** - Mult-IP's patented TCP/IP optimization, data compression algorithms, and exclusive modem integration all effectively combined to push more data across networks, improving performance on legacy systems and pulling more ROI from existing infrastructures.
- **Concurrent Networks** - Mult-IP's patented concurrent networks technology enables administrators to create multiple independent communication networks in one VPN, achieving an ideal balance between coverage, performance, control, reliability and cost.
- **Load-balancing and Scalability** - Mult-IP can scale in-service from a single gateway supporting several hundred users to multiple gateways supporting thousands of simultaneous users without impacting active sessions. On connection, new clients are automatically connected to the gateway with the lightest load.
- **Application and Session Persistence** - Mult-IP's automatic network reconnection ensures continuous connectivity by automatically and seamlessly reconnecting clients to the network when signal interruptions occur without any loss of data. Overcoming the loss of data associated with connectivity challenges, Mult-IP maintains an open socket connection to the network, giving session persistence and keeping applications running smoothly and continuously. Furthermore, application data is buffered, allowing connections to resume seamlessly following gaps in wireless coverage.
- **Split Tunneling** - Clients bypass the Mult-IP VPN for pre-defined applications (such as local printer or Internet browsing) when security is not required. It also prevents clients from repeatedly connecting and disconnecting to access resources on separate networks.
- **Group Policy Management** - Mult-IP's advanced Group Policy Management feature facilitates fleet distribution and management through configurable groups of clients, authentication type and application policies. It allows the IT administrator to control which application is used by a specific group of users and on which network.
- **Authentication, Encryption and Security** - Mult-IP exceeds the FBI CJIS and HIPAA requirements, providing FIPS 140-2, AES and 3DES encryption, supporting 2-factor authentication and meeting audit functionalities. Mult-IP also supports multiple administrators and various user levels to enable easy sharing and comprehensive access over a single distributed system.
- **Targeted Remote Updates** - The remote update functionality sends Mult-IP Client updates directly to selected field devices using the most cost-effective network resource available. Networks configuration may differ from one group to the other, meeting the needs of different groups as far as expected field conditions, known device tolerance, and so on.
- **Redundancy and Disaster Recovery Support with No Single Point of Failure** - Mult-IP provides the highest level of reliability via automated and synchronized replication of data between all gateways in a farm. Should one gateway fail or shut down for maintenance purposes, the client re-connects to the other available gateway(s). This type of redundancy is ideal for disaster recovery planning as the gateway farms can be installed in different geographic locations allowing for continuous operation in the event of a disaster.

- **Reporting** - The Mult-IP Analytics data collection option produces comprehensive reports providing IT administrators the necessary intelligence for immediate decision making and future planning.

System Topology

The following layout provides a functional view of the Mult-IP load-balancing topology. Customer preference for a single-gateway or load-balancing solution is usually established on the fleet size, expected traffic load or operational subdivisions within the organization.

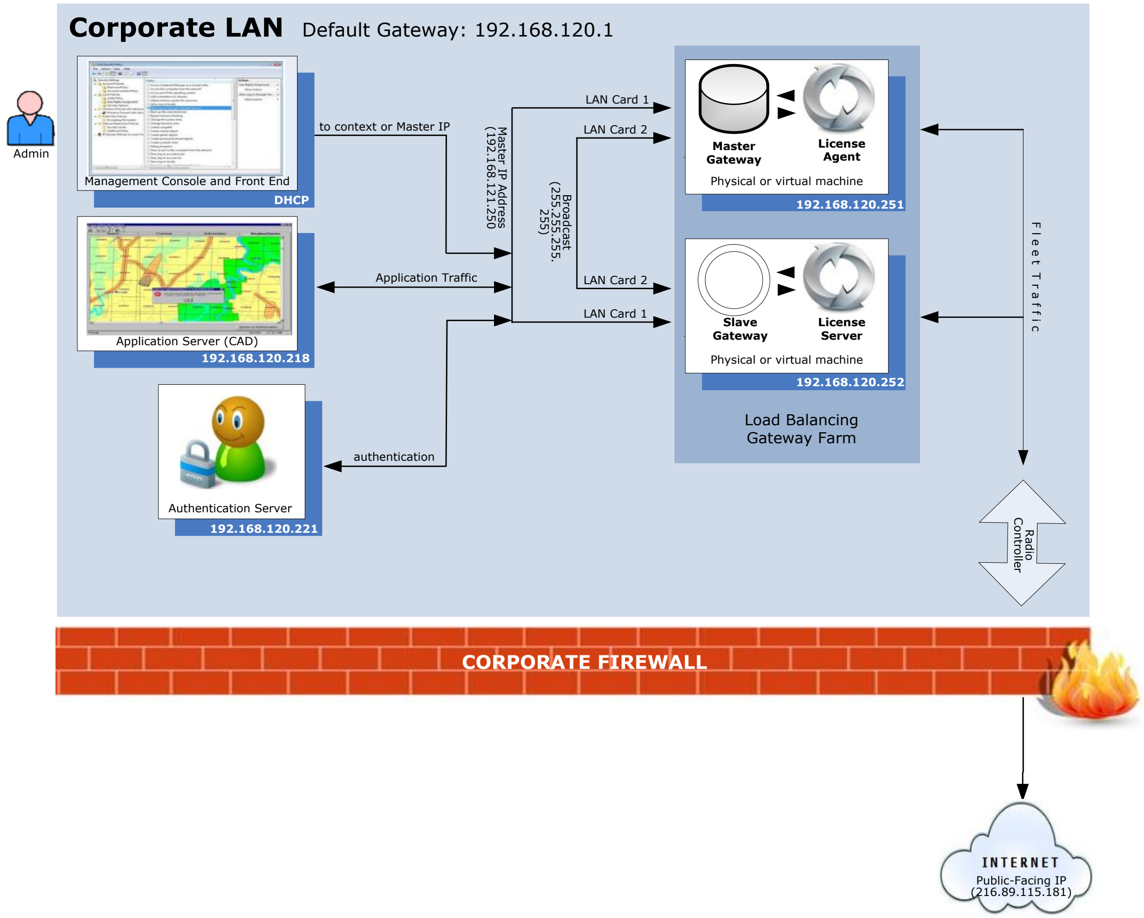


***Figure 1**: Load-balancing functional diagram*

The Mult-IP environment distributes routing effort across several components, drastically increasing transmitted data throughput, overall performance, management flexibility and system-wide reliability over an expanding fleet. The following sub-sections describe each component of the Mult-IP communication chain.

Mult-IP Gateways

Mult-IP is a fully scalable solution designed to distribute fleet traffic on two or more gateways linked together to form a load-balancing network. Each gateway runs as a background service receiving configuration commands and other queries from a Front End service acting as the middleware between gateways and management console conveniently located throughout the organization’s LAN.

In routine operation, Mult-IP Gateways handle traffic from a fleet of clients to LAN-based application servers or Internet services. As a scalable solution, Mult-IP offers three types of gateway topologies:

- In **single** mode, a single gateway is used to process traffic while the supplied VNIC (Virtual Network Interface Card) manages client addresses on a virtual IP segment isolated from the physical LAN as well as traffic to and from the outside world. The gateway also stores policy data such as communication driver definitions, group assignments, authentication methods as well as management console roles and user definitions.
- In a **load-balancing** configuration (figure 1), two or more gateways essentially share the same information, working together to distribute traffic based on incoming client connections (keep in mind that individual gateways still require a minimum amount of specific settings). However, a client connecting to a gateway will remain bound to it for the duration of its work session or until connection is reset, regardless of traffic. Meanwhile, additional clients may be routed to the next available gateway upon establishing connection in an effort to distribute traffic and mitigate excess load. To support a load-balancing solution, the **Radio IP Election Module** background service running on all Mult-IP Gateway hosts comes into play and literally assigns or “elects” one of the live gateways as master, effectively putting it in charge of gateway resources. While they continue handling fleet traffic, all remaining gateways are considered “slave”.
- The **Disaster Recovery** option gives you the possibility to setup a Mult-IP Recovery environment in a geographically separated site. In the Disaster Recovery (DR) scenario, gateways located at the recovery site are configured to be operational but run in standby mode awaiting manual activation. The Disaster Recovery (DR) gateways are intended to ensure continuity of operations in the event of a disaster at the main location of the master/slave gateways.

Gateway Resources

Whether configured in single or load-balancing mode, the Mult-IP mobile VPN solution relies on the following components, managed by the master Mult-IP Gateway:

- **Master IP Address:** Physical static IP address used to route traffic from application servers to the Mult-IP virtual IP segment. The master IP address acts as a return path for packets sent back to mobile devices.
- **Virtual Network Interface Card**: the VNIC acts as the point of entry/exit between the virtual IP segment and the corporate network. The VNIC card is active only on the master gateway.

The Front End Service

This service, installed alongside the management console, connects the console to all gateways in the same context. The Front End monitors gateway parameters and statuses at regular intervals and refreshes the management console with current data on the selected node.

The Management Console

The Mult-IP management console is a Microsoft® Management Console (MMC) snap-in that connects to a Front End service for interfacing with one or multiple gateways. While single-gateway mode is more permissive in allowing the console to run on the same machine as the gateway, the requirement of keeping the management console isolated from the gateway component stands out in a load-balancing environment because of the importance of minimizing the risk of accidental system access or excessive CPU load on gateway machines busy handling heavy traffic.

Typically, system administrators (or personnel with sufficient access rights) use the management console to remotely provision and manage groups of mobile clients, and to monitor gateways status. Mobile client provisioning employs configuration payloads defined using console tools and stored as policies shared on all gateways. Policies are applied to mobile clients whenever they register to the group for which those policies were defined. Policies include (but are not limited to):

- Client communication driver settings
- Packet Manager settings
- Concurrent network distribution (pipe and Roaming Profile definitions)
- Filter settings (filters consist of rules which help shaping traffic in order to prioritize particular data over a given network)
- Authentication method

Mult-IP Client

This client software is a small footprint service providing mobile workstations with concurrent-network VPN connectivity over an expanding range of wireless networks. The installer is supplied to mobile workstations via removable media or can be downloaded from a network location. It includes minimal connectivity settings for communication drivers and IP routes. Upon successful connection to the gateway, clients are quarantined until they are acknowledged by the system administrator operating the console and moved to a functional group where they immediately download policies assigned to that group.

In the field, end-to-end communication makes use of Radio IP's optimized wireless TCP/IP protocol, which exhibits the following behavior:

- Before leaving the client workstation, data packets are compressed while maintaining their QoS values
- Unnecessary overhead is removed and a trimmed header is created (instead of the usual 60-byte header)
- Radio network confirmation is used instead of TCP/IP confirmation when available
- Data travels to the radio controller via antenna
- Once information reaches the Mult-IP Gateway, the data stream is reconstructed in the correct order by applying the transport mechanism used on the client side in reverse order

Navigating the User Interface

The management console's graphical user interface (GUI) is at the heart of the Mult-IP Mobile VPN solution and acts as the main access point into the system from an administrative standpoint. Administrators use it to manage gateways and a fleet of mobile workstations.

The management console is designed to provide users with a flexible interface from which to perform a wide range of tasks ranging from system configuration and data filtering to real-time network monitoring and troubleshooting. Comprehensive role and responsibility management is also enforced at logon in order to protect your entire Mult-IP Mobile VPN against tampering.

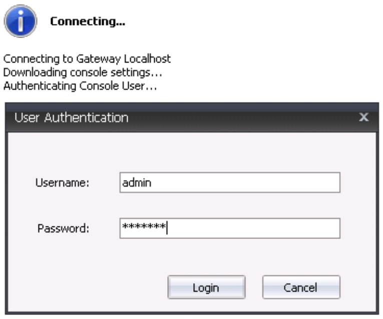
The Mult-IP management console is packaged as a snap-in that plugs into the Windows OS-supplied Microsoft® Management Console (MMC). You have the option of installing the console on any gateway machine or MMC 3.0-equipped standalone workstation connected to the physical LAN.

The next section describes how the Mult-IP snap-in enhances the MMC console with views (or workspaces) specific to the selected node. Each node will be reviewed individually.

Launching the Mult-IP management console

To launch the management console,

1. Double-click the desktop icon or point to **Start** > **All Programs** > **RadioIP** > **Mult-IP Management Console** > **Management Console**.
2. Wait for the login prompt after launch, an indication that the console has successfully connected to a Mult-IP Gateway.



Connecting...

Connecting to Gateway Localhost
Downloading console settings...
Authenticating Console User...

User Authentication

Username: admin

Password: *******

Note: Keep in mind that you will be prompted to personalize administrative credentials as part of the first login attempt.

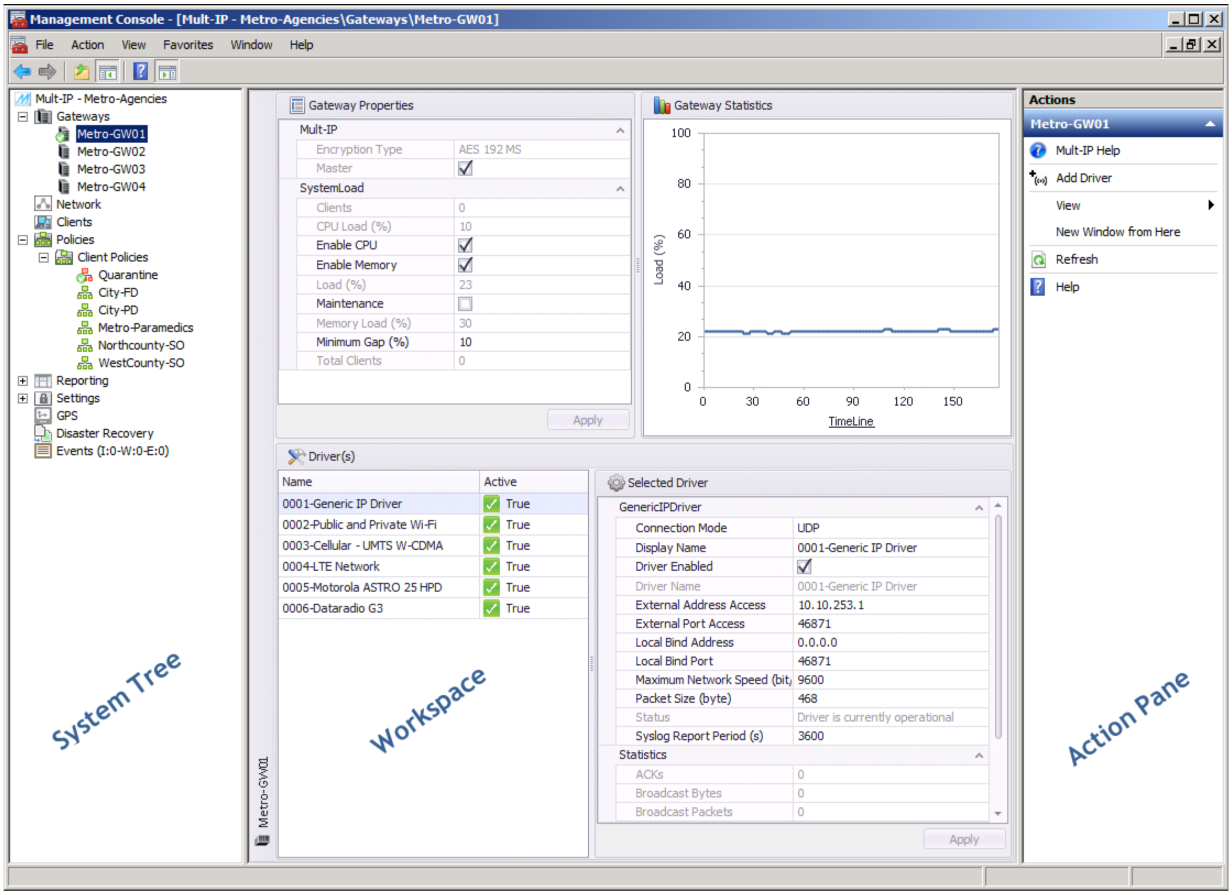
Note: Three failed attempts to log in will lock the user account. You will need to close the console and re-open it to get three more attempts.

Note: A connection error will ensue if you are launching the console without first applying the alternate connection method introduced during console installation.

Management Console Layout

The management console UI is divided into three main areas:

- The **System Tree:** The leftmost tree structure expands into sets of nodes, where each node defines a functional area of the Mult-IP system.
- The **Workspace**: As the name suggests, the area at the center of the console window features both display-only and editable attributes of the selected node. Tabs and portlets are often used to facilitate navigation to subsets of related parameters.
- The **Actions** pane: The rightmost area of the console window lists all context-sensitive actions available for the selected node. Note that the very least, the **Actions** pane replicates the contextual menus obtained when right clicking a node.



Gateway Properties

Mult-IP	
Encryption Type	AES 192 MS
Master	☑
SystemLoad	
Clients	0
CPU Load (%)	10
Enable CPU	☑
Enable Memory	☑
Load (%)	23
Maintenance	□
Memory Load (%)	30
Minimum Gap (%)	10
Total Clients	0

Driver(s)

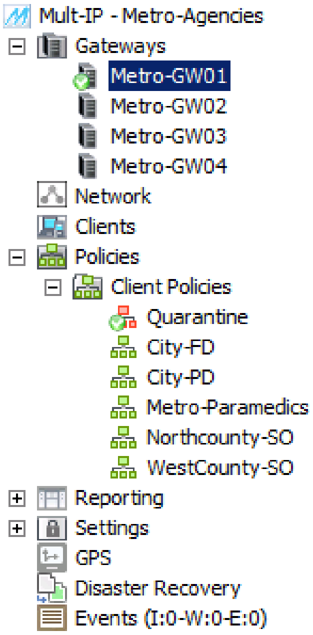
Name	Active
0001-Generic IP Driver	✓ True
0002-Public and Private Wi-Fi	✓ True
0003-Cellular - UMTS W-CDMA	✓ True
0004-LTE Network	✓ True
0005-Motorola ASTRO 25 HPD	✓ True
0006-Dataradio G3	✓ True

Selected Driver

GenericIPDriver	
Connection Mode	UDP
Display Name	0001-Generic IP Driver
Driver Enabled	☑
Driver Name	0001-Generic IP Driver
External Address Access	10.10.253.1
External Port Access	46871
Local Bind Address	0.0.0.0
Local Bind Port	46871
Maximum Network Speed (bit/	9600
Packet Size (byte)	468
Status	Driver is currently operational
Syslog Report Period (s)	3600
Statistics	
ACKs	0
Broadcast Bytes	0
Broadcast Packets	0

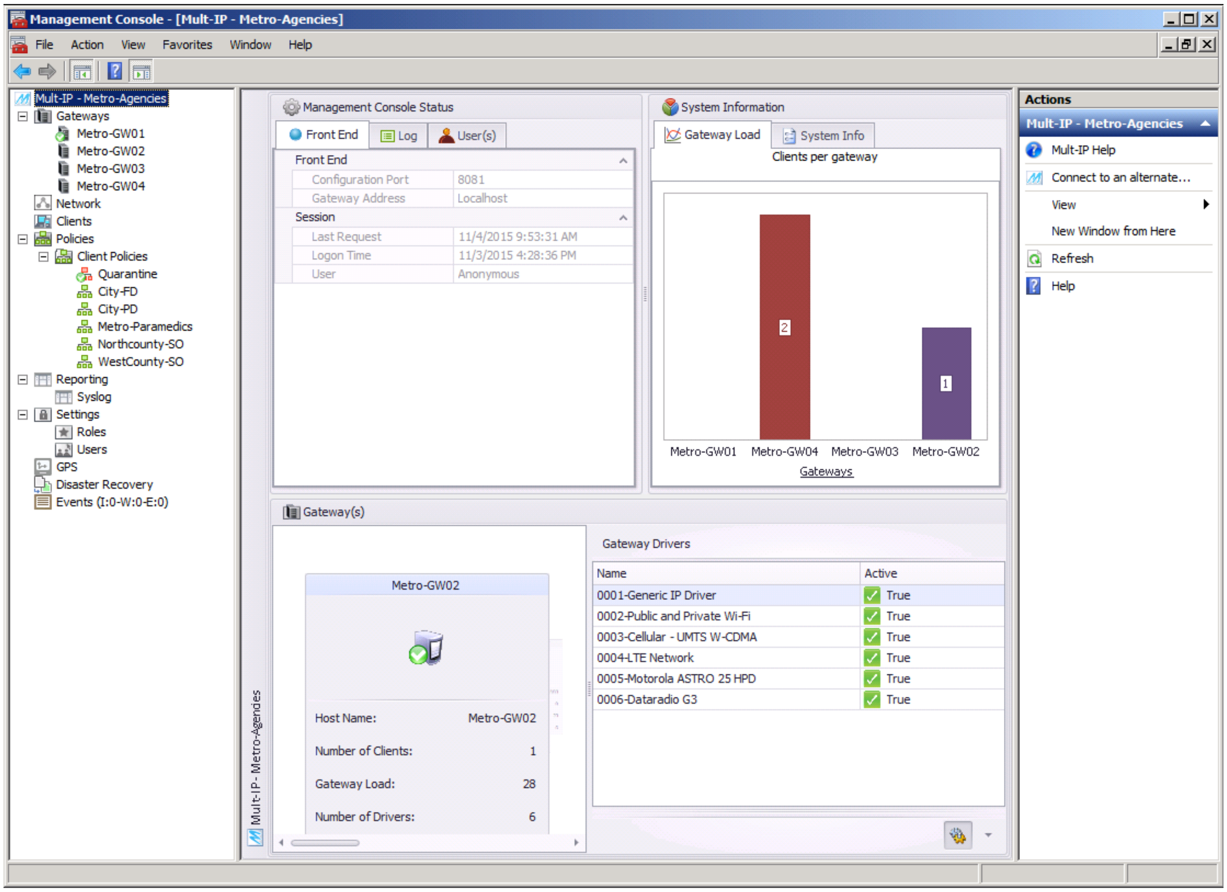
System Tree

As is it the case with typical MMC views, the Mult-IP system is arranged in an expandable tree structure. Here is a typical example of what a five-agency public safety organization structure could look like when managed by four load-balancing Mult-IP Gateways.



Mult-IP Dashboard

The Mult-IP Dashboard is located in the main workspace. It appears at launch or whenever the **Mult-IP** root node is highlighted.



Front End

Configuration Port	8081
Gateway Address	Localhost

Session

Last Request	11/4/2015 9:53:31 AM
Logon Time	11/3/2015 4:28:36 PM
User	Anonymous

Metro-GW02

Host Name:	Metro-GW02
Number of Clients:	1
Gateway Load:	28
Number of Drivers:	6

Gateway Drivers

Name	Active
0001-Generic IP Driver	✓ True
0002-Public and Private Wi-Fi	✓ True
0003-Cellular - UMTS W-CDMA	✓ True
0004-LTE Network	✓ True
0005-Motorola ASTRO 25 HPD	✓ True
0006-Dataradio G3	✓ True

This workspace is intended for monitoring convenience and provides a continuously updated display of system-wide activity. The view will keep refreshing with updated data for as long as the console remains connected to the same context. The Mult-IP Dashboard is display-only and is divided in the following four resizable panes:

- **Management Console Status** - The **Front End** tab displays static parameters about end-to-end lifeline connection between management console, Front End and gateway(s). The **Log** tab lists in-session status messages useful for on the spot troubleshooting. The **User(s)** tab identifies all users currently logged to the same gateway network context.

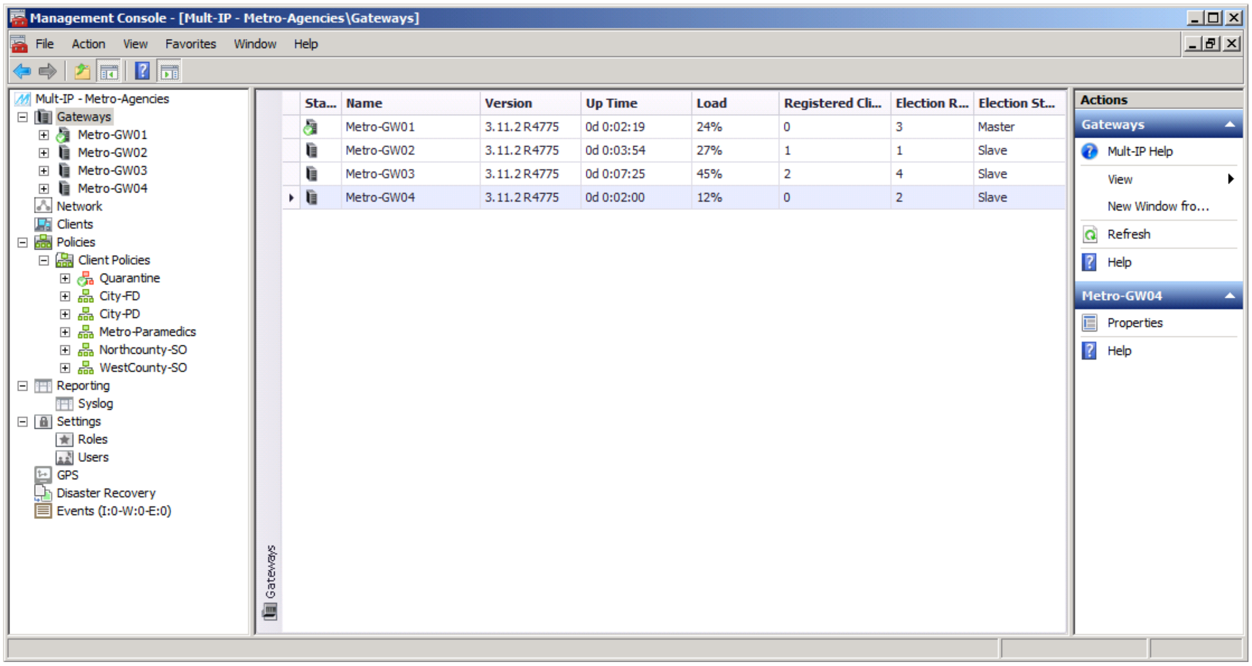
- **System information** - The **Gateway Load** tab provides an estimation of system load by way of live bar graphs. Use the scroll wheel of your pointing device to zoom in on the X-Y axis for finer variations over time, or zoom out for a broader view, useful for trending. This feature makes it easy to assess individual gateway load for a large fleet distributed over several gateways (in a load-balancing environment). The **System Info** tab identifies network context name, a reference to the type of encryption in use total client count and number of connected gateways.
- **Gateway(s)** - shows parameters specific to the gateway in the foreground, including the current number of registered clients. In a load-balancing environment, use the horizontal scrollbar to toggle between gateways.
- **Gateway Drivers** - lists all currently installed gateway communication drivers. In a load-balancing system, this list applies to all gateways. Active communication drivers are tagged with a green ✓ icon, while configured but inactive drivers are tagged by a red ⚠ icon.

Here is the description of the fields to be found in the Mult-IP Dashboard:

Field header	**Description**
Management Console Status – Front End tab	
Configuration Port	Port used for console control access to gateways.
Gateway Address	Gateway front end address on which the console is bound to.
Last Request	Time of the last user activity on the console.
Logon Time	Time of the current session logon.
User	User currently logged in the console.
System Information – System Info tab	
Context	Mult-IP context monitored.
Encryption Type	Type of encryption as defined by your system product license.
Total Clients	Total number of clients currently registered on all gateways.
Total Gateways	Number of active gateways in the context.

Gateways Node

The **Gateways** node lists all connected gateways:



Sta...	Name	Version	Up Time	Load	Registered Cli...	Election R...	Election St...
	Metro-GW01	3.11.2R4775	0d 0:02:19	24%	0	3	Master
	Metro-GW02	3.11.2R4775	0d 0:03:54	27%	1	1	Slave
	Metro-GW03	3.11.2R4775	0d 0:07:25	45%	2	4	Slave
	Metro-GW04	3.11.2R4775	0d 0:02:00	12%	0	2	Slave

This node displays the gateway status icon, name, installed version number, up time, current load and number of active clients registered to the gateway.

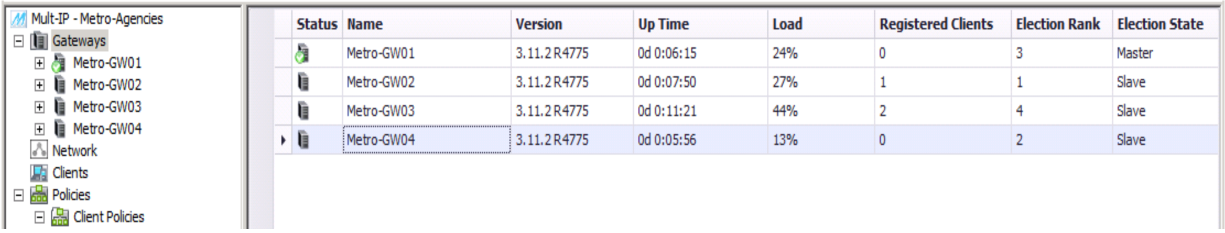
Here is a description of the icons used to display gateway status:

Icon	Description
✓	Master: The gateway is active and has been elected as master (or is the only gateway in the setup)
▮	Slave: The gateway is active but is not master.
✗	Unavailable: The gateway is inactive (machine shut down, Mult-IP service stopped, network issues)

Election state shows the current state (Master, Slave, Down or Missing Dependencies) for each gateway of the context

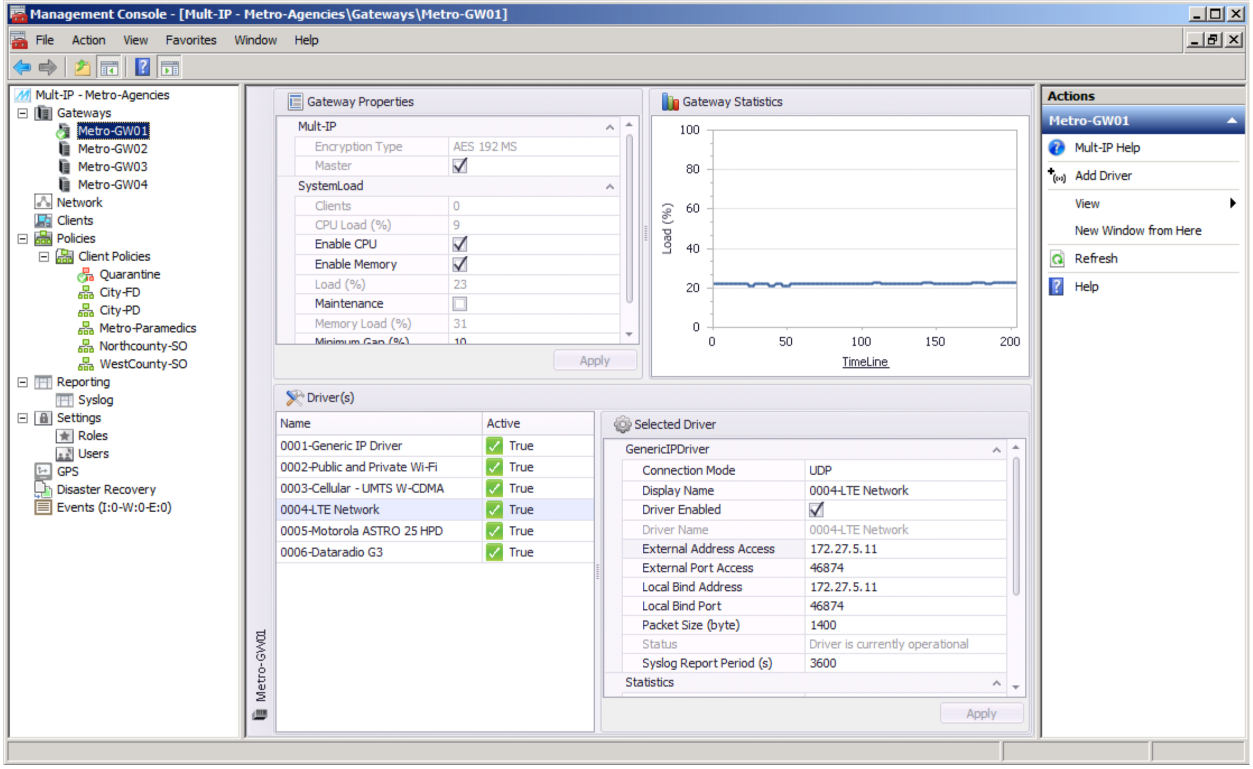
Election rank give the priority of each gateway to become master as per the Election procedure. When an election is triggered, the gateway having the highest available index and having the mandatory dependencies available becomes Master.

Note: When a gateway goes into maintenance mode, it is only indicated in the displayed name:



Status	Name	Version	Up Time	Load	Registered Clients	Election Rank	Election State
	Metro-GW01	3.11.2 R4775	0d 0:06:15	24%	0	3	Master
	Metro-GW02	3.11.2 R4775	0d 0:07:50	27%	1	1	Slave
	Metro-GW03	3.11.2 R4775	0d 0:11:21	44%	2	4	Slave
	Metro-GW04	3.11.2 R4775	0d 0:05:56	13%	0	2	Slave

Double-click a gateway or select **Properties** from the Actions pane to display, or click a gateway's machine name in the system tree to display the four-area workspace, with information focused on the selected gateway:



Mult-IP

Encryption Type	AES 192 MS
Master	☑

SystemLoad

Clients	0
CPU Load (%)	9
Enable CPU	☑
Enable Memory	☑
Load (%)	23
Maintenance	☐
Memory Load (%)	31
Minimum Gap (%)	10

Name	Active
0001-Generic IP Driver	✓ True
0002-Public and Private Wi-Fi	✓ True
0003-Cellular - UMTS W-CDMA	✓ True
0004-LTE Network	✓ True
0005-Motorola ASTRO 25 HPD	✓ True
0006-Dataradio G3	✓ True

GenericIPDriver

Connection Mode	UDP
Display Name	0004-LTE Network
Driver Enabled	☑
Driver Name	0004-LTE Network
External Address Access	172.27.5.11
External Port Access	46874
Local Bind Address	172.27.5.11
Local Bind Port	46874
Packet Size (byte)	1400
Status	Driver is currently operational
Syslog Report Period (s)	3600

Statistics

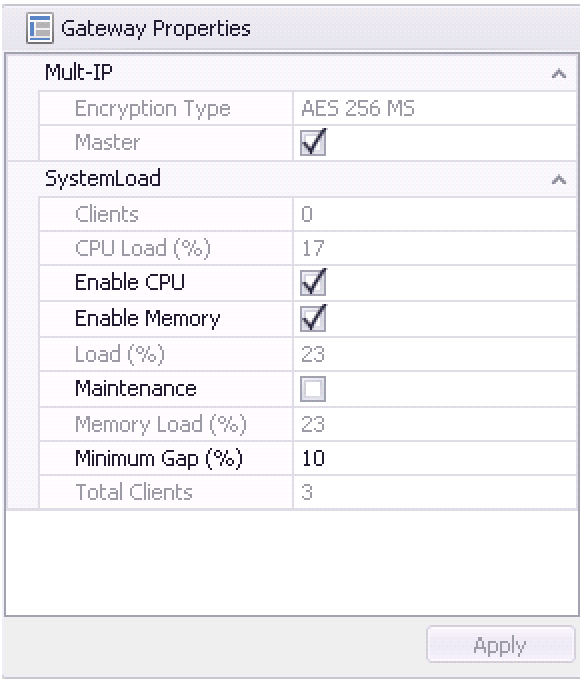
Upper areas show gateway properties and real-time gateway dashboard load useful for trend analysis. Bottom area displays gateway communication drivers complete with editable parameters. Note that while displayed information applies to the selected gateway, most editable parameters will apply across all gateways in a load-balancing environment.

Select a gateway node to add communication drivers. Later in the process, the same drivers can be customized to the requirements of selected functional groups.

Notice that enabled communication drivers are tagged with a green ✓ icon while configured but disabled drivers are tagged with a red ⚠ icon.

If you are running a load-balancing solution, all gateways share the same communication driver definitions with the notable exception of the External Address Access, Local Bind Address and the External port access parameters which require attention

Below is a detailed view of the gateway properties part:



Gateway Properties

Mult-IP	
Encryption Type	AES 256 MS
Master	☑
SystemLoad	
Clients	0
CPU Load (%)	17
Enable CPU	☑
Enable Memory	☑
Load (%)	23
Maintenance	☐
Memory Load (%)	23
Minimum Gap (%)	10
Total Clients	3

Table 1: Gateway properties

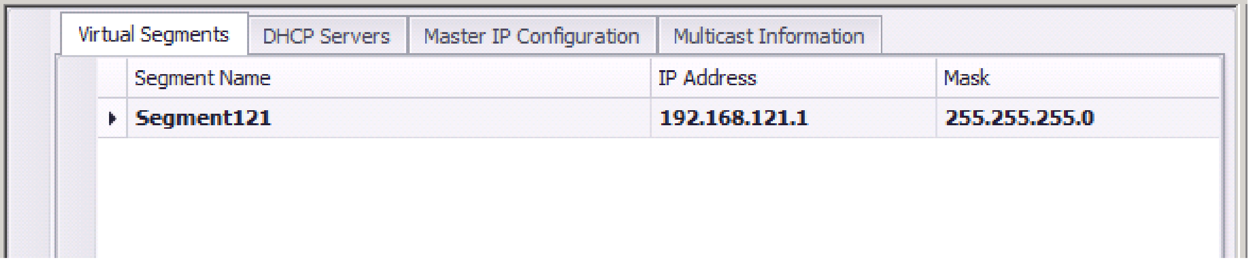
Parameter	**Description**
Mult-IP	
Encryption Type	Type of encryption as defined by your system product license.
Master	Indicates whether the selected gateway is running as a master (checked) or a slave (unchecked). While all load-balancing gateways are equally responsible for handling client traffic, the master gateway is the only one managing gateway resources.
System Load	
Clients	Total number of clients currently registered on this gateway.
CPU Load (%)	A read-only indication of the relative stress put on the local host CPU. This value is used for performance comparison purposes between gateways of a given load-balancing farm.
Enable CPU	Check box so that CPU usage is taken into account when calculating the selected gateway's ability to accept mobile client connections. Enabling this parameter may prevent machine with limited CPU capacity or machines running multiple applications from accepting a high volume of client connections. This applies to all gateways.

Parameter	Description
Enable Memory	Check box so that memory usage is taken into account when calculating the selected gateway's ability to accept mobile client connections. This parameter may prevent machines with limited RAM from accepting a high volume of client connections. This applies to all gateways.
Load (%)	A read-only indication of the relative usage (in %) of the selected gateway machine which takes into account the number of mobile clients, CPU usage (if enabled) and memory usage (if enabled).
Maintenance	Check box to divert reset mobile client connections to other available load-balancing gateways. In doing so, gateway connections will progressively decrease to a point where no mobile client is connected, allowing you to put the gateway offline for a planned outage without impacting fleet operation. See also Maintenance mode.
Memory Load (%)	Percentage of machine memory currently being used by the selected gateway.
Minimum Gap (%)	Sets a minimum acceptable load delta between the highest-load gateway and the others in a load-balancing environment. If this gap exceeds the value, new registrations will be handled by the lowest-load gateway. By default, set to 10%. This applies to all gateways.
Total Clients	Total number of clients currently registered on all gateways.

The Network node

This multi-tab node encompasses items related to network configuration. In it, you have access to Mult-IP virtual segments, DHCP servers IP and the master IP configuration.

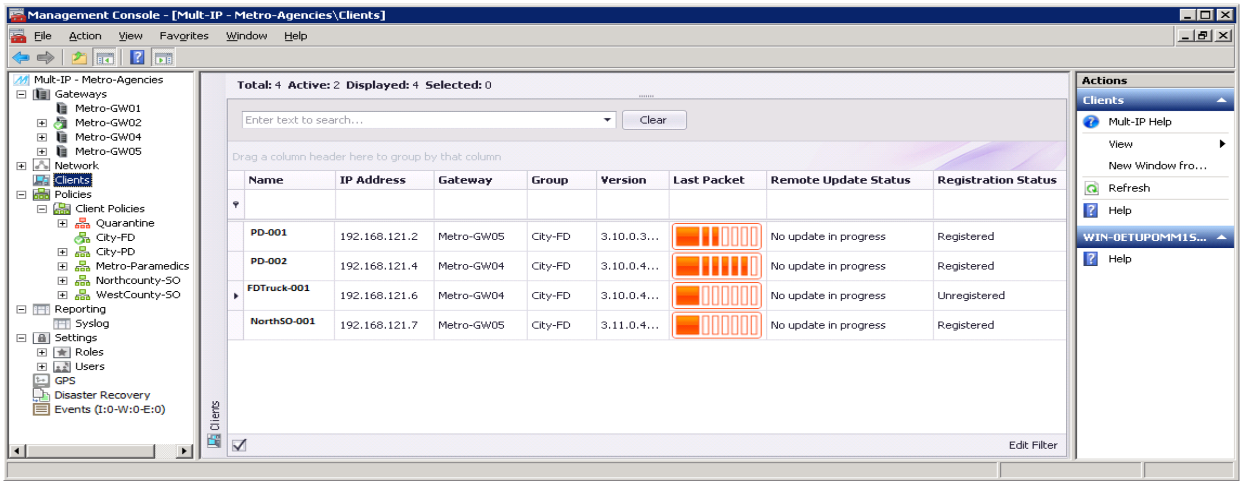
⚠	**Warning** After the first gateway installation, it is mandatory to configure at least one virtual segment, one DHCP server IP address and the master IP address for the system to be operational.



Segment Name	IP Address	Mask
Segment121	192.168.121.1	255.255.255.0

Clients Node

The **Clients** node lists all clients currently existing(both quarantined and registered) to any Mult-IP Gateway in the same context. Use this view to query client status information and to assign clients to groups. A summary status bar displays the total number of clients in the list, as well as the number of active (registered) clients and the number of selected clients. A search bar allows system administrator to retrieve one or more mobiles in the fleet, for which any item in the client properties matches the entered string pattern.



Total: 4 Active: 2 Displayed: 4 Selected: 0

Name	IP Address	Gateway	Group	Version	Last Packet	Remote Update Status	Registration Status
PD-001	192.168.121.2	Metro-GW05	City-FD	3.10.0.3...		No update in progress	Registered
PD-002	192.168.121.4	Metro-GW04	City-FD	3.10.0.4...		No update in progress	Registered
FDTruck-001	192.168.121.6	Metro-GW04	City-FD	3.10.0.4...		No update in progress	Unregistered
NorthSO-001	192.168.121.7	Metro-GW05	City-FD	3.11.0.4...		No update in progress	Registered

Displayed information includes:

- **Name**: actual client machine name, customizable via the Windows OS Computer Name option.
- **IP address**: this field shows the current (in use) IP of the client.
- **Gateway**: identifies the gateway on which the client is connected. This is useful in a load-balancing environment.
- **Group**: Identifies the group on which clients are assigned. Initially, clients appear in the *Quarantine* group where they remain in a minimal connection state until they are acknowledged. This column is especially useful while the fleet is being assembled; it allows operators to distinguish quickly quarantined clients and clients assigned to their respective functional group.
- **Version**: Lists the four-part version number of the Mult-IP Client software running on registered mobile workstations. This information assists in the management of the Remote Update feature.
- **Last Packet:** This column provides an indication of the cumulative time elapsed since packets were last received in the form of a six-level bar graph. Level indicators report as follows:

Last Packet	Rx State threshold
▮▮▮▮▮▮▮	0 = less than 15 seconds ago
▮▮▮▮▮▮▯	1 = between 15 and 45 seconds
▮▮▮▮▮▯▯	2 = between 45 seconds and 1 minute 15 seconds
▮▮▮▮▯▯▯	3 = between 1 minute 15 seconds and 2 minutes 15 seconds
▮▮▮▯▯▯▯	4 = between 2 minutes 15 seconds and 4 minute 15 seconds
▮▮▯▯▯▯▯	5 = between 4 minutes 15 seconds and 14 minutes 15 seconds
▮▯▯▯▯▯▯	6 = more than 14 minutes 15 seconds

- **Remote Update status**: this column provides information about Mult-IP software updates as per the published version in the functional group. It allows the system administrator to follow the progress of remote patching. The following are the possible statuses:
  - **No update in progress** - means that the mobile runs an up to date version of Mult-IP as per its group policies;
  - **Downloading in progress .. 50%** - means that a client is currently downloading the published version and the percentage informs of the progress;
  - **Downloaded** - means that the published package was fully downloaded and the mobile is currently installing the update. This status will change to "**No update in progress**" after the next client registration.
- **Registration status**: this column provides information about the current registration status of a client (registered/unregistered).

Additional columns are also available in the column chooser dialog. These columns are intended for troubleshooting:

- **Client ID and Mac Address**: allow to find a specific mobile that requires maintenance
- **IP Status**: this column shows the current IP status of a client. The following are the possible statuses:

  - **IP status "N/A"** means the client did not registraed to the gateway since the last sytem start-up.
  - **Dynamic** - means that a client receives a dynamic IP address from the DHCP server;
  - **Renewal Timeout** - means a response from the DHPC server to a DHCP request was not received in a timely fashion and a client is not registered;
  - **Static** - means that the IP address is provided directly by the client and the Mult-IP Vnic adaptor is set with an IP Address in static mode.
- **Operating System**: this column shows the operating system that is in use by each client and it may be helpful during a troubleshooting session.
- **Policies schema number:** this column shows the current Policies schema number (version) used by a client. If it does not match the publishing number in the Group configuration, the client is not up to date. A reset connection then forces this client to register and retrieve the latest version of the group policies.

Customizing Viewing Preferences

The Clients view supports column reordering as well as list sorting and filtering to accommodate viewing preferences. Customizing this view can prove especially useful when browsing through an extensive list of mobile clients.

To reorder columns,

To change the order in which columns are displayed, simply click and drag individual columns over adjacent column boundaries. Reordering does not affect sorting order unless such order is manually changed.

To sort columns,

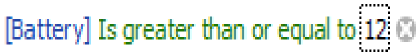
- Click-hold a column header and drag leftmost to sort the entire client list according to that criterion. Click the up or down arrow to change sorting in ascending or descending order.
- Click-hold a column header and drag upward into the column group area. Doing so will round up all clients according to the dragged criterion in a collapsed (but expandable) state. Use this grouping method to distribute clients by functional group, or in a load-balancing environment, to view clients registered to individual gateways. Keep in mind that you can drag several columns where each one is treated in descending order of precedence.

To sort item within a column,

Set the focus on the column header, just below the column title, and enter a string pattern you are looking for. Column is then automatically restricted to the items including the searched pattern.

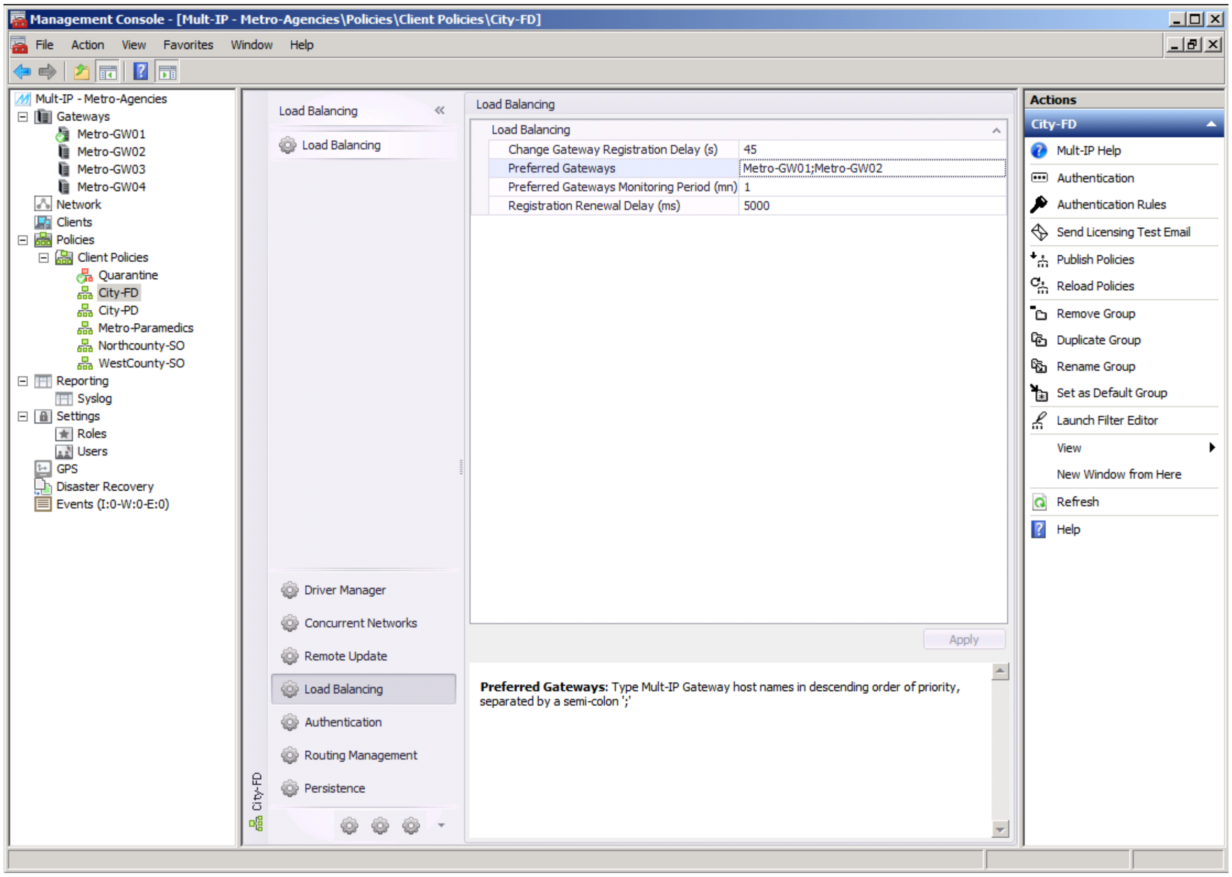
Additional management options

Right clicking a column header reveals additional column management options by way of the following context menu items:

Menu item	Description
Sort Ascending	Perform an ascending sort order of the selected column.
Sort Descending	Perform a descending sort order of the selected column.
Clear Sorting	Revert client list viewing state to the state prior to the last applied column filter.
Group by this column	Force client grouping by the selected column
Hide Group By Box	Reduce clutter of client view by collapsing the “Group by” area.
Remove This Column	Remove the selected column. Click Column Chooser to add column.
Column Chooser	Display a floating window listing all hidden columns. Right-click individual columns to show or drag to desired column position.
Best Fit	Widen the selected column to show display unit in full.
Best Fit (all columns)	Resize all columns according to character width.
Clear Filter	Clear column filter by restoring previous view.
Column Filter	Display a conditional filter window. Use it to formulate and implement a simple or complex filter string by comparing two or more conditions to a selected argument of type “And”, “Or”, “Not And”, “Not Or”. Click the insert (+) switch to add a condition to the string. Click the “X” switch to delete condition. Notice that you may refine the scope of individual conditional elements by tagging it with an argument and specifying inclusive or exclusive values. For example, to display only those mobile device with minimum amount of battery life, you might set an argument as follows:  [Battery] Is greater than or equal to 12 ⊗ Where 12 represents the percentage (%) of battery left.

The Client Policies Node

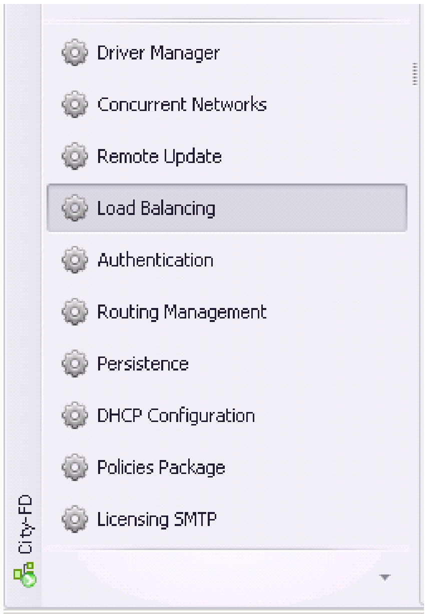
Expand the **Policies** node to reveal **Client Policies**, the area that requires most administrative attention. Its primary purpose is to manage the fleet by defining, and then provisioning client groups with communication driver settings, roaming profiles, authentication schemes, etc.



Change Gateway Registration Delay (s)	45
Preferred Gateways	Metro-GW01;Metro-GW02
Preferred Gateways Monitoring Period (mn)	1
Registration Renewal Delay (ms)	5000

Preferred Gateways: Type Mult-IP Gateway host names in descending order of priority, separated by a semi-colon ';'

Each functional group contains clients' sharing characteristics ranging from common hardware to agency distribution, such as the ones shown above. Each functional group features a multi-tab portal with settings applicable to all clients of that group, regardless of its size:



As will be discussed later, access to this area should be restricted to users with a thorough understanding of client communication driver configuration.

- Click **Driver Manager** to enable or disable communication drivers, or to edit settings that better reflect hardware specifications, radio coverage or other field conditions.
- Click **Concurrent Networks** to set roaming profiles based on one or several communication drivers. Once published, each profile relies on the wireless system (or communication driver) best suited for the type of data routed to the selected pipe. Note that one roaming profile can be customized for each pipe you wish to assign to specific data usage, such as video, voice or text. Pipes are designed to optimize the use of narrowband versus broadband data. For instance, this level of flexibility allows network administrators to channel voice communications over private narrowband networks while routing video conferencing or email attachment download to broadband networks such as cellular or Wi-Fi.
- Click **Remote Update** to remotely update the Mult-IP Client application on all mobile workstations of the selected group. Keep in mind that remote updates are transferred over **Pipe3**. See Remote Update for feature description.
- Click **Load-balancing** to set the basic parameters of a load-balancing solution. Of particular interest to the system administrator, this tab defines a list of gateways in descending order of priority mobile devices will attempt to connect to in the event of an out-of-coverage situation.
- Click **Authentication** to access information on authentication method configured for that group.

- Click Routing Management to access the specific routes and routing management sub-tab feature which allows clients of the selected group to simultaneously access public networks and corporate LAN resources using the same physical connection.
- Click **Persistence** to set a gateway's ability to monitor a registered client's in-coverage status at the session and application levels, and to automatically allow clients back on the network with no need to register after a failure in communication lasting no more than preset durations.
- Click DHCP Configuration to assign a predefined virtual address scope to the clients of the selected functional group along with a selected DHCP server. If it's not customized, the default value is used.
- Click Policies Package to view information about the latest successful group policy publishing. This information allows detecting clients, which are not running the latest policies version.
- Click **Licensing SMTP** to set up unattended forwarding of license-related alarms to email recipients.

The Reporting Node

Access the Reporting node to set system event destination to one of two possible external options. On the one hand, you may install the Mult-IP Analytics add-on and retrieve comprehensive system data in the form of detailed Excel charts. On the other hand, rely on the built-in Syslog option to retrieve system events locally (CSV format) or route data to a third-party Syslog appliance. Go to **Reporting System Events** to review and set reporting options.

The Settings Node

This functionality allows administrative personnel to build various roles on the basis of granting or denying display/editing permissions to any or all management console configuration and monitoring areas.

Roles can be assigned to as many users as you wish to allow in the system either by rank (such as *admin*, *user*, *guest*, and so on) or by actual user names. Roles and users apply to console administration and define how one is empowered to interact with the system.

Keep in mind that role and user partitioning data is stored at the system level and equally applies to all gateways in the same load-balancing environment. Therefore, an organization supporting several independent Mult-IP systems would be required to define sets of roles and users for each system.

Refer to Applying Console Security for more information.

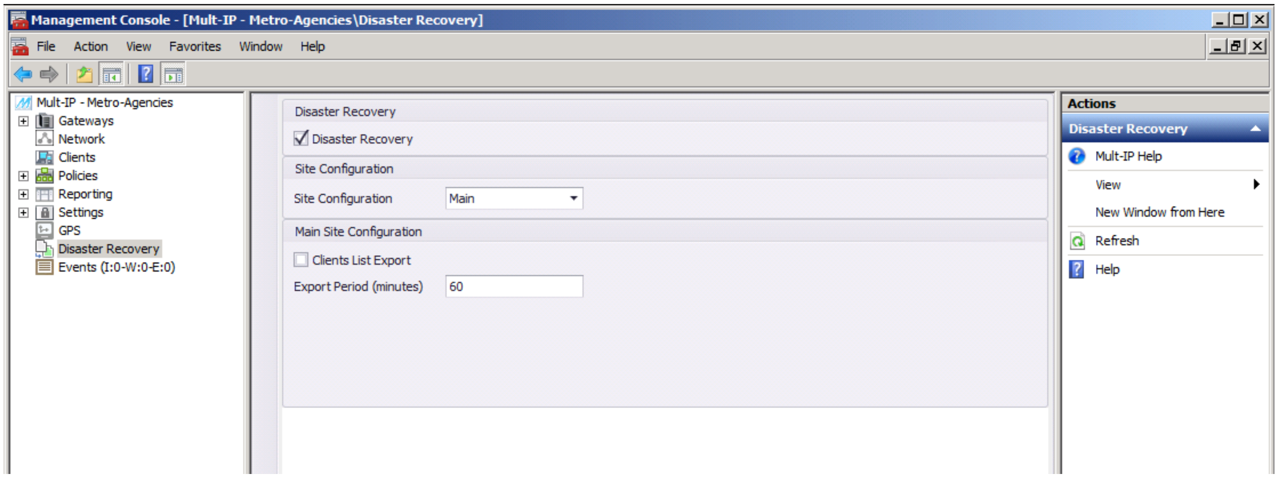
The GPS Node

This node allows enabling and configuring access to the Radio-IP GPS Director. To do so, select Enable, click Apply and set the IP address and the port to communicate with the GPS Director's Mult-IP extension. Make sure to pay attention to your local firewall rules.

Disaster Recovery Node

This node allows access to the Disaster Recovery configuration. To configure the disaster recovery, start by enabling the Disaster Recovery mode. Then from the drop down list, select Main site or Recovery site depending on your location.

Main site configuration only requires setting a timer for the client data export frequency. Only the necessary information for the DR registration is exported for the client to register. The timer values range from 1 to 60 mn, the default value for an efficient yet not excessive backup.



Management Console - [Mult-IP - Metro-Agencies\Disaster Recovery]

Disaster Recovery

☑ Disaster Recovery

Site Configuration

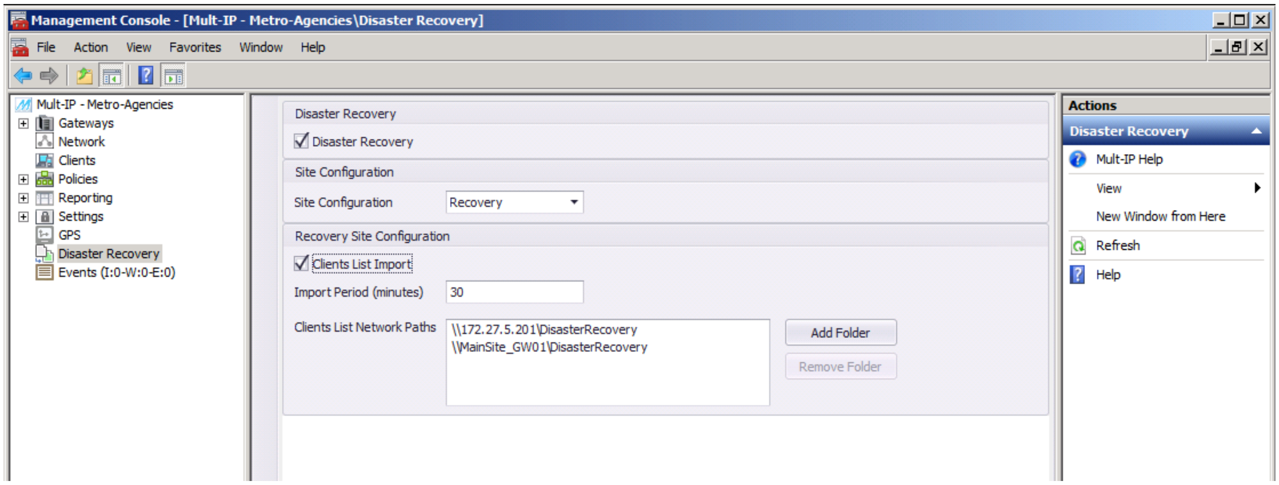
Site Configuration: Main

Main Site Configuration

□ Clients List Export

Export Period (minutes): 60

Recovery site configuration requires setting timer frequency to retrieve client data from the main site and the path to the network share to the Disaster Recovery folder for each gateway located at the main site.



Management Console - [Mult-IP - Metro-Agencies\Disaster Recovery]

Disaster Recovery

☑ Disaster Recovery

Site Configuration

Site Configuration: Recovery

Recovery Site Configuration

☑ Clients List Import

Import Period (minutes): 30

Clients List Network Paths:
\\172.27.5.201\DisasterRecovery
\\MainSite_GW01\DisasterRecovery

This process is simple yet efficient and reliable. The configuration file of the main site is replicated to the Disaster Recovery site at intervals set by the user. In the event when the main site becomes unavailable as a result of a disaster, the communication between Mult-IP clients and the gateways on the Recovery site (for example, open or redirect firewall rules or enabling a driver) should be opened manually. Pre-provisioned dedicated DR-address driver (lower priority) on clients will ensure automatic connectivity to the new master gateway at the DR site. After the registration to a DR gateway, clients are provided with a specific set of policies as defined by the DR site configuration.

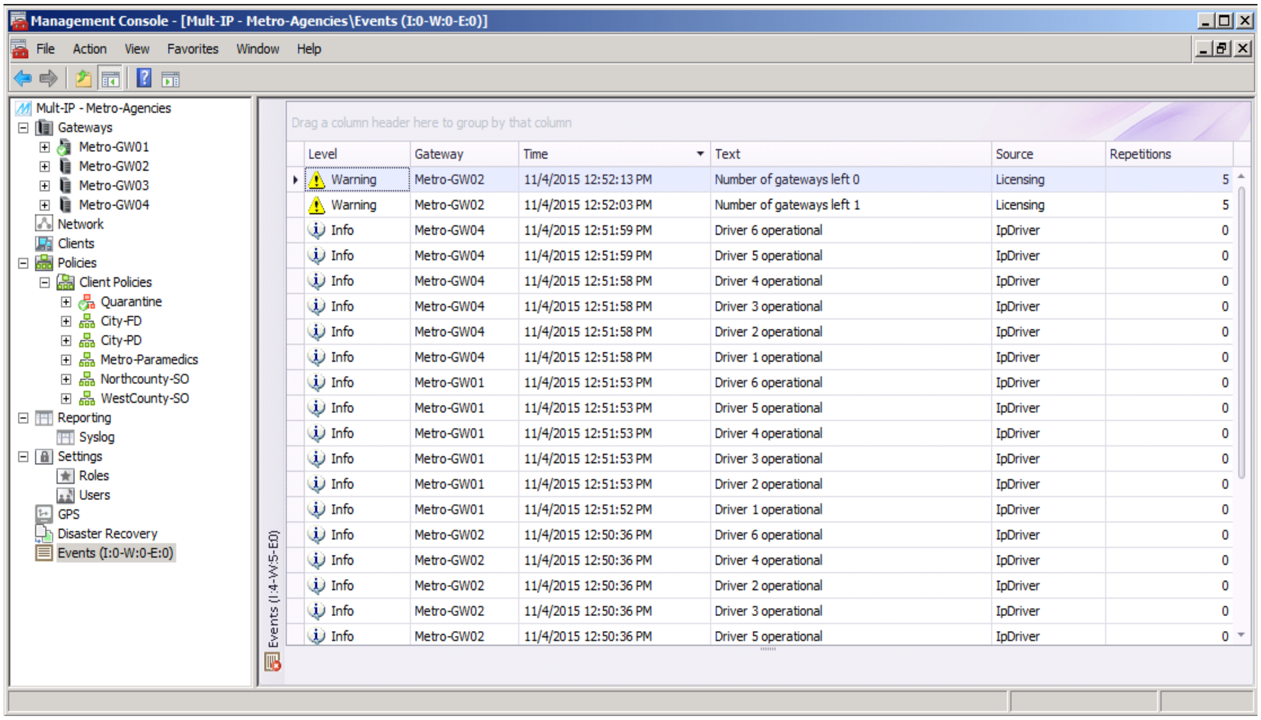
Events Node

The **Events** node collects short-term data information about system status and helps the end user operating the Management Console to troubleshoot eventual issues.

Here is the description of the icons used to display the status:

Icon	Description
▤	No new Error/Warning events logged since the last time Events node was accessed
▤✖	New Error/Warning events logged since the last time Events node was accessed. Your attention is required.

Use this view to query the last system events generated within the same context.



Level	Gateway	Time	Text	Source	Repetitions
Warning	Metro-GW02	11/4/2015 12:52:13 PM	Number of gateways left 0	Licensing	5
Warning	Metro-GW02	11/4/2015 12:52:03 PM	Number of gateways left 1	Licensing	5
Info	Metro-GW04	11/4/2015 12:51:59 PM	Driver 6 operational	IpDriver	0
Info	Metro-GW04	11/4/2015 12:51:59 PM	Driver 5 operational	IpDriver	0
Info	Metro-GW04	11/4/2015 12:51:58 PM	Driver 4 operational	IpDriver	0
Info	Metro-GW04	11/4/2015 12:51:58 PM	Driver 3 operational	IpDriver	0
Info	Metro-GW04	11/4/2015 12:51:58 PM	Driver 2 operational	IpDriver	0
Info	Metro-GW04	11/4/2015 12:51:58 PM	Driver 1 operational	IpDriver	0
Info	Metro-GW01	11/4/2015 12:51:53 PM	Driver 6 operational	IpDriver	0
Info	Metro-GW01	11/4/2015 12:51:53 PM	Driver 5 operational	IpDriver	0
Info	Metro-GW01	11/4/2015 12:51:53 PM	Driver 4 operational	IpDriver	0
Info	Metro-GW01	11/4/2015 12:51:53 PM	Driver 3 operational	IpDriver	0
Info	Metro-GW01	11/4/2015 12:51:53 PM	Driver 2 operational	IpDriver	0
Info	Metro-GW01	11/4/2015 12:51:52 PM	Driver 1 operational	IpDriver	0
Info	Metro-GW02	11/4/2015 12:50:36 PM	Driver 6 operational	IpDriver	0
Info	Metro-GW02	11/4/2015 12:50:36 PM	Driver 4 operational	IpDriver	0
Info	Metro-GW02	11/4/2015 12:50:36 PM	Driver 2 operational	IpDriver	0
Info	Metro-GW02	11/4/2015 12:50:36 PM	Driver 3 operational	IpDriver	0
Info	Metro-GW02	11/4/2015 12:50:36 PM	Driver 5 operational	IpDriver	0

Displayed information includes:

- **Level**: Info, Warning or Error.
- **Gateway**: The gateway that generates the event.
- **Time**: Local time stamp of the event.
- **Text**: Message generated by the internal module/gateway
- **Source**: Internal module that generates the event.
- **Repetitions**: Number of occurrences since the previous event was displayed.

Message	Source	Level
License expired	RockCore	Error
License will expire in N days	Licensing	Warning
No communication with license server master for the last N days	Licensing	Warning
Number of gateways left N	Licensing	Warning
Percentage of the license used by clients reached N%	Licensing	Warning
Driver N not operational	IPDriver	Warning
Driver N operational	IPDriver	Information

Custom Actions

Each management console node is dedicated to a specific area of the Mult-IP environment, either for configuration or for in-service management and monitoring. This implies a certain number of custom actions performed either by invoking context-sensitive menus or by clicking items listed in the **Actions** pane (this area can be toggled on and off by clicking the ▤ toolbar icon). The next table lists the actions one is most likely to encounter while administering the Mult-IP Mobile VPN:

Table 2: Management console context-sensitive menu options

Node	Description
Root > **Connect to an alternate Front End**	Displays connection options to an alternate Front End service for connecting to a gateway network not specified during installation.
[**GatewayName**] > **Add Driver**	Adds a gateway communication driver. Driver can later be configured to the requirements of the entire fleet or to reflect hardware specifics of selected groups.
Network > [**Virtual segment**] > Add segment	Adds a virtual segment to be used by Mult-IP clients. This information should reflect the provisioning of DHCP segments on your DHCP server.
Network > [**Virtual segment**] > Edit segment	Edits a virtual segment: only a segment name can be modified.
Network > [**Virtual segment**] > Remove segment	Removes a virtual segment: this operation is only possible when a segment is released from a group assignment or if it is not the last one.
Network > [**Virtual segment**] > Set As Default Segment	Selects a segment and sets it as the default segment for the Mult-IP system. It is used by functional groups without a dedicated segment or it could be selected as a dedicated segment in a functional group
Network > [DHCP Servers] > Add DHCP	Adds a DHCP Server IP address along with a provider's name. You may want to use the provider in a functional group configuration to redirect the DHCP traffic to a dedicated DHCP server.
Network > [DHCP Servers] > Edit DHCP	Edits a DHCP provider:This will modify the IP address and the provider's name.
Network > [DHCP Servers] > Remove DHCP	Removes a DHCP server this operation is only possible when the DHCP server provider name is released from a group assignment or if it is not the last one.
Network > [DHCP Servers] > Set As Default DHCP	Selects a DHCP server and sets it as the default DHCP server for the Mult-IP system. It is used by functional groups without a dedicated DHCP server or it could be selected as a dedicated DHCP provider in a functional group
Network > Master IP	Sets the master IP and the subnet mask used by Mult-IP system.
Clients > [**ClientName**] > **Remove**	Removes the client from the client list. Client will reappear if it registers again.
Clients > [ClientName] > Reset Connection	Forces a client to register again, in order to download and apply the new set of policies, to force a change of gateway or to trigger a remote update.
Clients > [ClientName] Properties	Displays a multi-tab box. It contains specific information about this client
Clients > [**ClientName**] > **Assign to Group**	Allows the operator to move selected clients between groups. Especially useful to move clients from the *Quarantine* group to their target functional group. See also Processing New Client Connections**.**
Client Policies > **Add Group**	Creates a functional group whose purpose is to manage clients sharing common attributes (ex.: hardware or agency-related).
Client Policies > **Reset Default Group**	Resets the destination of all newly connected clients to the *Quarantine* group.
[**GroupName**] > **Authentication**	Defines the authentication method for clients of the selected functional group.
[GroupName] > Authentication Rules	Gives access to the Authentication Rules manager. It is used to manage (add, remove, edit, activate.) the authentication rules for a group

Node	Description
[GroupName] > **Send Licensing Test Email**	Validates the configuration with a mail server.
[GroupName] > **Publish Policies**	Saves changes made to one or to several group parameters. Published policy information is stored in the gateway and is transferred to clients of the target group the next time they are assigned or registered to the target group.
[GroupName] > **Reload Policies**	Updates the current view with the last changes saved in gateway storage. As a general rule, updates are grayed out to be limited to display-only parameters, preserving locally edited parameter(s).
[GroupName] > **Remove Group**	Deletes the selected group. In doing so, all clients registered to this group will return to the *Quarantine* group (or user-assigned default group) when they reconnect. You cannot delete a group if clients are assigned to this group. See also Processing New Client Connections.
[GroupName] > **Duplicate Group**	Creates a copy of the selected group. The user will be prompted to enter the name of the new group. When duplicating a group, some of the original Specific Routes might not be copied. It is important to check the routes in the newly created group and add the ones that are missing manually to complete the duplication.
[GroupName] > **Rename Group**	Displays the Rename Group dialog used to edit a group name.
[GroupName] > **Set as Default Group**	Defines the functional group as the default destination for new client connections (instead of the *Quarantine* group by default). Upon initial connection to the Mult-IP network, clients automatically join the default group by downloading policies defined for this group. Clients will remain assigned to the default group until a console operator redirects them to another functional group. This feature is especially useful when a large number of mobile clients is expected to connect.
[GroupName] > **Launch Filter Editor**	Brings up the Filter Editor wizard. Use it to define the rules, which control the handling of the application packets (allowed, blocked or dropped).
Reporting > Open Analytics Library	Starts the Analytics tool (if installed), designed to collect short-term and long-term data into detailed reports useful for system analysis, trending and auditing.
Settings > **Export List…**	Exports the list of custom-defined users and roles to a text file. Useful in a large organization for traceability or auditing purposes.
Settings > Change Password	Brings up the change password box. Use it to change the password of the current user
Roles > **Add Role**	Defines a role by selecting items from a list of access rights.
Roles > **Access Rights**	Defines the rights to display and allows modifying information in different nodes in the Mult-IP console.
Roles > **Group Assignment**	Defines the visibility of group policies for this role.
Roles > **Duplicate Role**	Duplicates a role. This action is especially useful when, for instance, you want to duplicate the same permissions to all group-level administrative roles.
Roles > **Delete Role**	Deletes a role, provided there is no user assigned to it.
Users > **Add User**	Creates a new user, by defining a username, a password and a role.
Users > **Edit User**	Allows changing a user’s password or a role assignment.

Node	Description
Users > **Delete User**	Deletes a user.

Note: The access rights for the user's role define the visibility of these context-sensitive menus.

System Operation

The operational topics discussed in this section are presented in the order in which they should be approached from the standpoint of a new Mult-IP solution deployment. They are designed to help you grasp the logical chain of activities to be performed when deploying a fully functional Mult-IP Mobile VPN. Beware that rapid product evolution will most likely impact some of the topics described next.

To deploy your Mult-IP environment,

- apply management console security;
- Prepare the gateway to manage client registration;
- add and configure gateway communication drivers;
- configure client communication drivers;
- create the functional groups in which your mobile workforce will be distributed;
- define Roaming profiles;
- define filter rules;
- configure client policy payload;
- register and assign clients to functional groups;
- monitor system and provision clients with policy updates.

Note: Avoid using any of the special characters listed in Appendix C - Predifined XML Entities while editing the text-entry fields used at various stages of your configuration. These characters are reserved for internal use only. Here a table summarizing the naming rules you should follow:

Rules	Scope	Groups	Context	Roles	Users	Password
Spaces	Allowed	Allowed	X	Allowed	X	X
Characters ! * & ' < > \ / “	X	X	X	X	X	X
Max length (characters)	40	40	40	128	40	20

Applying Console Security

The Mult-IP management console is the main interface used for system-wide configuration, monitoring and maintenance. Because of the possible implications of one’s actions on long term system stability, it is imperative that IT administrators implement security measures early on in order to restrict individual access to those assets he is called to manage. This holds especially true in large public service organizations where staff oversees several agencies over three or four work shifts.

Mult-IP provides the functionality to create and maintain roles and user profiles. Access data is saved in the Mult-IP Gateway(s), and is equally applied to all management consoles connected to the same context. This section discusses how an administrator chooses from a complete library of access rights, those that fit the requirement for a given role, which is then linked to individual users.

Roles

About this section:

To mitigate the risk of adversely affecting your Mult-IP environment, restrict management console to trained personnel. Rigorous role definition and their association to actual users address such concerns, giving the administrator more control over configuration of the Mult-IP environment for long-term stability and integrity.

A role is a collection of access rights granted to a user in the management console. Mult-IP comes preloaded with a single role - *SuperUser* - but the number of supported roles is limited only by the combinations of granted access rights and display/write permissions you wish to implement. To facilitate the task of defining access limitations to your VPN solution, consider the following typical role descriptions in their capacity to meet the requirements of most corporate settings:

- **SuperUser** - this built-in role has display/write access to all system areas and features. For example, the person holding the role of *SuperUser* can configure gateways, create groups, design and publish client policies. However, this role usually belongs to IT administrators in charge of delegating work among staff by designing subordinate roles.
- **GroupAdmin** - define this role to allow a remote IT employee to manage gateways, assign clients to the functional group(s) that fall under his corporate jurisdiction as well as to design group policies. The group administrator could also be allowed to add subordinate users to assist in the management of a large group.
- **Guest** - define a role that grants wide or narrow viewing rights to casual users, such as budget planners or decision-makers whose need is limited to monitoring the system in action.
- **Disabled** - define an “all access rights denied” type role assigned to users that will not be accessing the system for some extended period of time due to such factors as planned vacations or other extended leave of absence. This will help protect large corporations against identity theft.

Note: Mult-IP supplies a single built-in role known as SuperUser. This role is associated with the admin user. SuperUser role and admin user cannot be edited or deleted.

The system supports the principle of assigning a role to multiple users while each user holds a single role. Moreover, a role can be deleted at any moment as long as no users are linked to it.

Roles are based on trusted delegation: the concept of empowering users by assigning them responsibility over certain aspects of the overall solution. You are encouraged to create roles by selecting access rights that match specific tasks; such would be the case with group administration.

Note: An administrator might create another user having a role with higher rights.

Defining Roles

Roles exist to mitigate access to sensitive areas and as such, their definition is an important part of the Mult-IP administrator’s task.

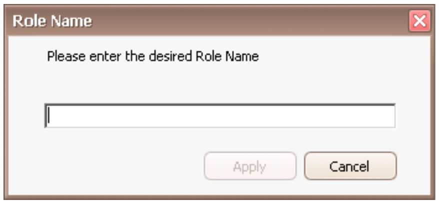
The first step in managing access to your Mult-IP environment using the management console requires that the administrator builds subsets of access rights in as many roles as are needed to cover all possible access conditions. As a best practice, Radio IP strongly encourages administrators to define all foreseeable roles before allowing users into the system.

Important notices:

- The role of *SuperUser* is built into the system and provides display/write permissions to all features. For security reasons, this role should be granted to administrative personnel only.
- Take some time to plan your role structure before defining it into the system. Once defined and linked to actual users, roles cannot be deleted unless users are deleted first.
- A Syslog message is generated whenever a role is created, edited or deleted.

To create roles,

1. Log on to the management console as a *SuperUser*.
2. Expand the **Settings** node, then right-click **Roles**.
3. Click **Add Role** from the context menu.



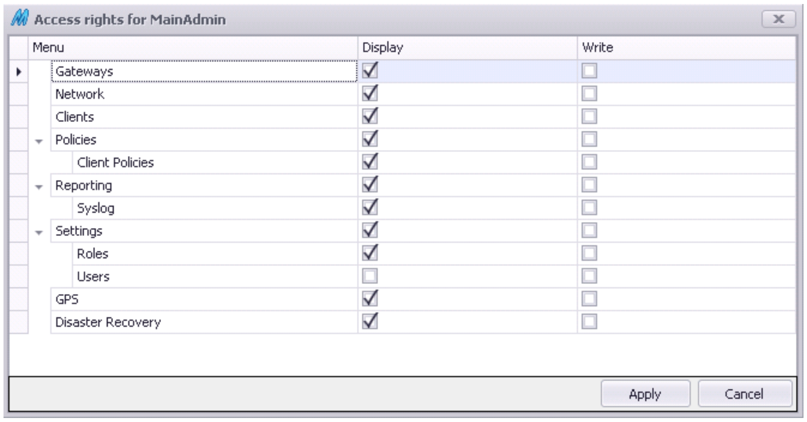
Please enter the desired Role Name

4. Type a string of characters to identify the new role, and then click **Apply**. Review Roles for a rundown of suggested nomenclature.

Note: Maximum length is 128 characters; spaces in role name are allowed but avoid special characters:

! * & ' < > \ / ”

5. Click to expand the tree structure. The view should look like this.



Menu	Display	Write
Gateways	☑	□
Network	☑	□
Clients	☑	□
Policies	☑	□
Client Policies	☑	□
Reporting	☑	□
Syslog	☑	□
Settings	☑	□
Roles	☑	□
Users	□	□
GPS	☑	□
Disaster Recovery	☑	□

Note: The access rights template is set to allow display and write permissions in all areas by default.

1. Browse the list of access areas and customize permissions for the *PoliceGroupAdmin* role (as per screen sample). For example:

a) Select **Gateways** and check *display* permission. This will allow the user associated with this role to review gateway communication driver settings for editing his assigned group's client communication driver settings whenever needed. Uncheck *write* permission to prevent accidental editing of sensitive gateway parameters.

b) Select **Clients** and check *display*. Uncheck *write* to prevent this group administrator to inadvertently move clients from one group to another.

c) Select **Policies** and check *display* / *write* permissions, allowing policy definition and publishing to clients of assigned groups.

d) Select **Reporting** and check *display* / *write* permissions to give access to system event destination and Mult-IP Analytics report queries.

e) Select **Settings** and uncheck *display*. In doing so, both permissions get unchecked, preventing this role from tampering with role and user definitions.

f) Select **GPS** and check *display* / *write* permissions to forward GPS coordinates received from clients to GPS director if necessary.

g) Select **Disaster Recovery** and check *display* / *write* permissions to configure both sites of the Disaster Recovery setup.

2. Click **Apply** when done.

Note: For a guest-level role, consider granting display rights (while denying write access) to most areas. Make sure to deny write access to the **Settings** node.

Notice the new *PoliceGroupAdmin* role appearing in the Roles workspace (center screen).

Editing Roles

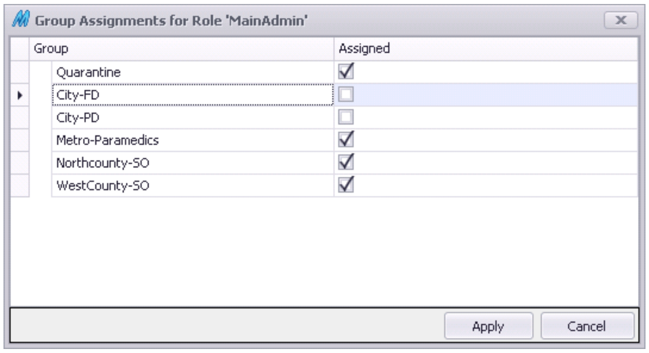
The following actions, visible in the Actions pane, can be performed on the selected role:

- **Access Rights:** to edit previously set permissions.
- **Group Assignment**: to select the group administered by the selected role. As a best practice, the role name should preferably depict the system object or client group it is designed to manage.
- **Duplicate Role:** to duplicate a generic role. This action is especially useful when, for instance, you want to duplicate the same permissions to all group-level administrative roles.
- **Delete Role**: to delete a role. Keep in mind that the built-in *SuperUser* role cannot be deleted.

Note: An existing role cannot be renamed.

To assign groups to a role,

Select the **Group Assignment** action in the action pane, the following dialog will appear, with all the groups unselected by default. Select all the groups that will be managed by the users in this role:



Group Assignments for Role 'MainAdmin'

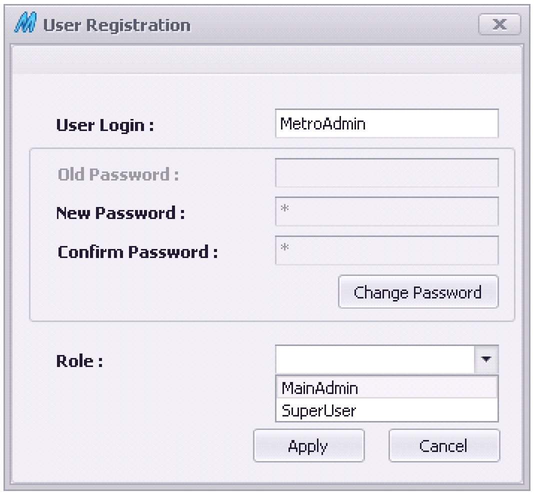
Group	Assigned
Quarantine	☑
City-FD	□
City-PD	□
Metro-Paramedics	☑
Northcounty-SO	☑
WestCounty-SO	☑

Creating and Managing Users

The task of managing users consists in linking user credentials to existing roles, resulting in a user profile. For accountability reasons, you are encouraged to limit the all-permissions *SuperUser* role to a small group of users.

To create users,

1. Log on to the management console as a *SuperUser* or as a user with sufficient privileges (display/write access to the **Settings** node).
2. Expand **Settings**, right-click **Users** and select **Add User** to view the User Registration window.



User Registration

User Login : MetroAdmin

Old Password :

New Password : *

Confirm Password : *

Role :

3. Add users as follows:
   a) Type a case insensitive **User login** name for the new user with a maximum length of 40 characters. Special characters ! * & ' < > \ /” and spaces are not allowed. For instance, you may type “john” or “johnsmith”, but not “john smith”.
   b) Type a case sensitive **New Password** for the new user with a minimum length of 8 characters and a maximum length of 20 characters. Special characters ! * & ' < > \ /” and spaces are not allowed.
   c) Confirm the password.
   d) Click the **Role** drop-down list and make a selection from the list of available roles. This selection is mandatory.

Each new user is added to the User Login workspace (center screen). The following actions, visible in the Actions pane, can be performed on the selected user:

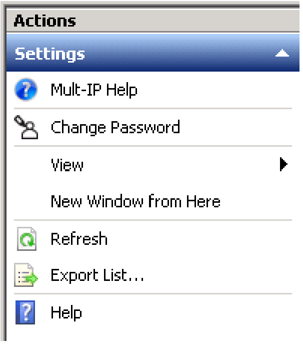
- Click **Edit User** to change user password and associated role.
- Click **Delete User** to delete entry and prevent user from further accessing the management console at the next logon attempt.

Note: The admin user is built-in and cannot be deleted.

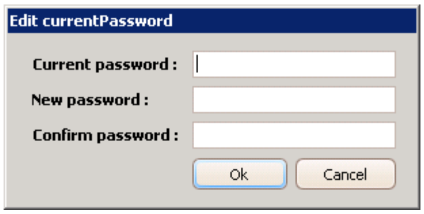
Note: As a known limitation, any user from a role created with display right on groups (and thus different from the SuperUser role) will only able to see groups that exist at the time of the creation of its role. All subsequently created groups will not be visible to that user.

To change user password,

Once logged in, a user can change his password by navigating to the **Settings** node (if its role has the display right on this node), and clicking on the **Change Password** item in the Action Panel:



A dialog is then prompted for password change:



Prepare the gateway to manage client registration

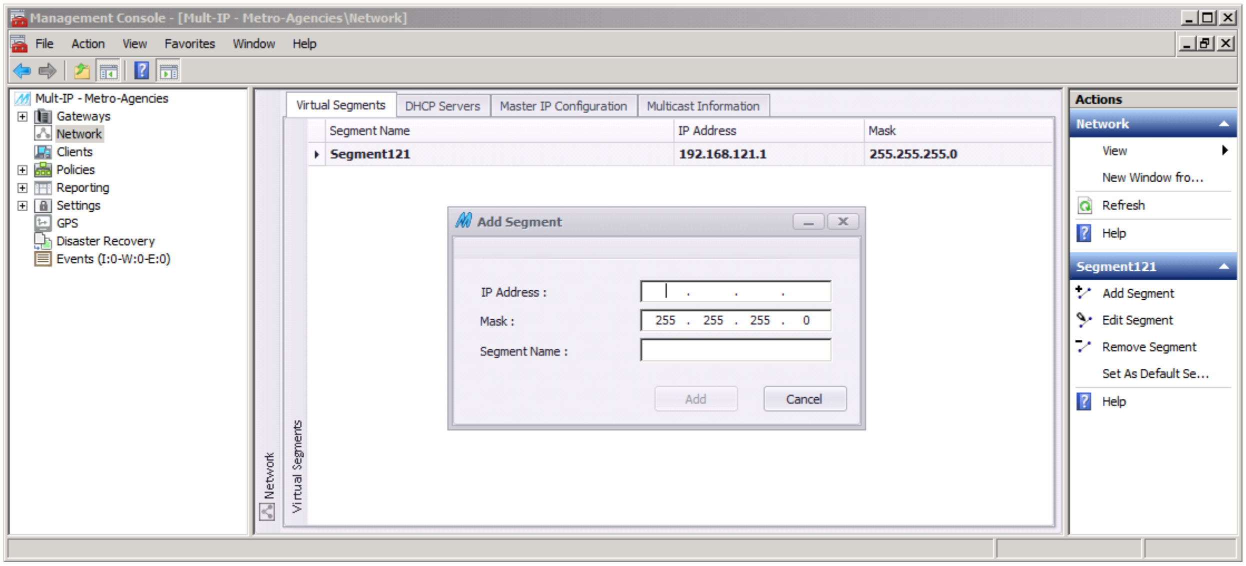
For the first gateway to be fully functional, several network options need to be set up in the Network Node.

Under the Virtual Segments tab, it is possible to add, edit or delete a virtual IP segment. The first added segment is the default one, unless another segment is added and selected. The default segment (always in bold) identifies the virtual IP segment that provides a pool of DHCP addresses for all functional groups which do not have an assigned custom segment.

When adding a segment, the selected IP address is used by the VNIC on the master gateway. Set the network mask and give a custom name to reflect your environment (optional). This will facilitate DHCP scope assignment later on. Scope name should be at most 40 characters long and not contain spaces nor special characters, such as ! * & ' <. > \ / “.

When editing a virtual IP segment, it is possible to change the segment name.

It is possible to delete a virtual segment if it is released from functional group assignment. However neither the default segment nor the last one can be deleted.


Management Console - [Mult-IP - Metro-Agencies\Network]

Segment Name	IP Address	Mask
Segment121	192.168.121.1	255.255.255.0

Add Segment

IP Address : . . .

Mask : 255 . 255 . 255 . 0

Segment Name :

The DHCP Servers tab allows to define the DHCP server IP address The DHCP server manages DHCP requests from Mult-IP. It is possible to configure one, two or more DHCP server IP addresses. It is also possible to give a custom name (provider name) to reflect your environment. Later it is also possible to assign a specific DHCP provider in a functional group.

Your work environment can be made more intuitive by setting a provider name. This provider name could be then selected in the functional group under the DHCP tab to forward any request from this group to this DHCP server specifically. This way it is possible to handle several agencies running with their own environment.

The third tab, Master IP Configuration, allows to define the master IP for Mult-IP system.

Adding and Configuring Gateway Communication Drivers

This highly technical aspect of the deployment process calls for system integrators to collect connection details for all public and private data communication systems accessible to fleet clients and compile this information in a pre-install checklist. While small-scale organizations can limit the scope of their configuration effort to simple off-the-shelf wireless solutions such as WI-FI or public cellular, large scale deployments require extensive knowledge of private mobile radios (PMR) to effectively set such parameters as packet size and compression.

On the gateway side, integrators must plan for possible roaming scenarios. Considering that Mult-IP Gateways act as a single point of entry into the corporate LAN, they must contain communication driver definitions for any communication method at the disposal of any one client in the fleet.

Each client must be provisioned with communication drivers that address the characteristics of the local machine. For example, if your organization relies on two wireless networks, then only two network-specific drivers will need to be defined and enabled on the gateway. However, for clients supporting only one of those networks, then administrators can issue policies containing a single driver definition. Keep in mind that Mult-IP allows you to “fine tune” communication drivers configured on the gateway at the functional group level, allowing you, for example, to apply one or several settings specific to hardware only found on clients of a given group.

Supported communication drivers

The following table lists communication drivers with default values for all public and private wireless systems supported as of publication of this documentation. Notice that Mult-IP divides drivers into the following tiers: **Basic** and **Premium** to reflect the extent of your product license. Keep in mind that **Premium** communication drivers are optional.

Table 3: Supported communication drivers

Driver Name	Packet Size (Bytes)	Connect Speed (Bits/sec)	Mode
Basic (public and private mobile networks)			
Cellular - CDMA2000 1xEVDO Rev A	1400	2500000	UDP
Cellular - CDMA2000 1xRTT	1400	300000	UDP
Cellular - CDMAOne	1400	0 (unlimited)	UDP
Cellular - GSM	1400	0 (unlimited)	UDP
Cellular – GSM CSD	1400	0 (unlimited)	UDP
Cellular – GSM EDGE	1400	250000	UDP
Cellular – GSM GPRS	1400	115000	UDP
Cellular – GSM HCSD	1400	0 (unlimited)	UDP
Cellular – IP Mobilenet	512	25000	UDP
Cellular – UMTS HSPA	1400	1100000	UDP
Cellular – UMTS W-CDMA	1400	140000	UDP
Dataradio CPhr	1400	0 (unlimited)	UDP
DataRadio G3	1450	43200	UDP
Esteem IP	1400	0 (unlimited)	UDP
Generic IP	1024	0 (unlimited)	UDP
Harris OpenSky	512	7200	UDP
Harris P25	300	2400	UDP
IDEN	1400	0 (unlimited)	UDP
LTE Network	1400	0 (unlimited)	UDP
Mesh Alvarion	1400	0 (unlimited)	UDP
Mesh GE MDS (for Net II modem family)	2048	10000000	UDP
Mesh GE MDS (for Mercury 900 modem)	4096	20000000	UDP
Mesh Tropos Metromesh	1400	0 (unlimited)	UDP
Motorola ASTRO 25 HPD	1430	90000	UDP
Motorola ASTRO 25 Trunked IVD (IV&D)	480	9600	UDP
Motorola EVDO	1370	0 (unlimited)	UDP
Motorola LTE BC 13	1370	0 (unlimited)	UDP

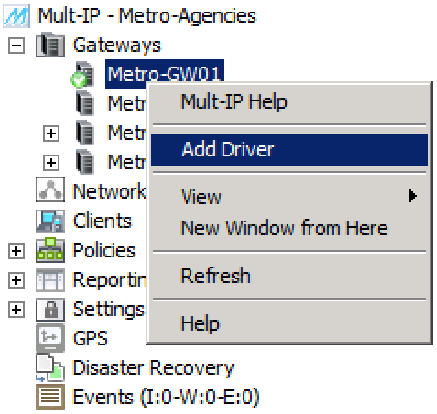
Driver Name	Packet Size (Bytes)	Connect Speed (Bits/sec)	Mode
Motorola LTE PSST	1370	0 (unlimited)	UDP
Motorola MotoMESH	1400	0 (unlimited)	UDP
Motorola Wi-Fi	1370	0 (unlimited)	UDP
Novaroam	1400	0 (unlimited)	UDP
Public and Private Wi-Fi	1024	0 (unlimited)	UDP
Standard Dialup IP Network	1024	57600	UDP
TETRA	1400	4000	UDP
WiMax	1400	0 (unlimited)	UDP
Premium (private mobility network)			
Motorola DataTAC	This is a non-IP driver. Set parameters to local hardware preferences.		
DataRadio G2 (not supported in LB mode)	This is a non-IP driver. Set parameters to local hardware preferences.		

Enabling Gateway communication drivers

For the benefit of our sample scenario, let us add a communication driver (in addition to the default Generic IP driver packaged with the system). Subsequently, a policy update will be issued and pushed to clients as they connect to the system, allowing them to use the new communication driver functionality in the field.

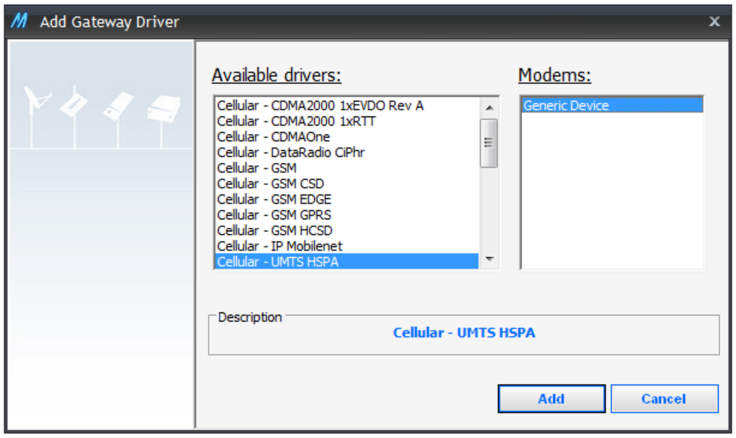
Note: Mult-IP ships with a pre-configured Generic IP driver on both gateway and client. This default is suitable for first-time client registration over wireless (Wi-Fi) or wired LAN. Do not disable or make changes to this communication driver since it is intended as a lifeline to field workers called to restore client software to factory defaults.

To configure and enable a gateway communication driver,



1. As shown, browse the system tree, and expand the **Gateways** node and right-click a gateway. In a load-balancing environment, select the master gateway highlighted by a ( ) icon. Saved settings will then propagate to all other gateways.

2. Click **Add Driver** from the context menu to bring up the Add Gateway Driver wizard.



Add Gateway Driver

Available drivers:

Cellular - CDMA2000 1xEVDO Rev A
Cellular - CDMA2000 1xRTT
Cellular - CDMAOne
Cellular - DataRadio CiPhr
Cellular - GSM
Cellular - GSM CSD
Cellular - GSM EDGE
Cellular - GSM GPRS
Cellular - GSM HCSD
Cellular - IP Mobilenet
Cellular - UMTS HSPA

Modems:

Generic Device

Description: Cellular - UMTS HSPA

3. Select the communication driver that best matches the type of wireless network you wish to add, then point to a supported modem. Note that the vast majority of drivers will list supported modem as “Generic Device” which fits the requirements for most hardware manufacturers.
4. Click **Add** and complete the communication driver setup wizard. Refer to the next table for parameter description.

Note: By default, the newly added communication driver will appear in a disabled state as evidenced by a red ⚠ icon.

5. Review parameter values In the **Selected Driver** area of the gateway workspace. Make appropriate change, such as **External Address** and **Local Bind Address** then click **Apply** to update system.

Note: Pay special consideration to parameters such as **Packet Size** and **Connection Speed**. Always set to the advertised performance of the wireless network and local hardware. Avoid entering erroneous values as this may overburden the network and adversely affect data throughput.

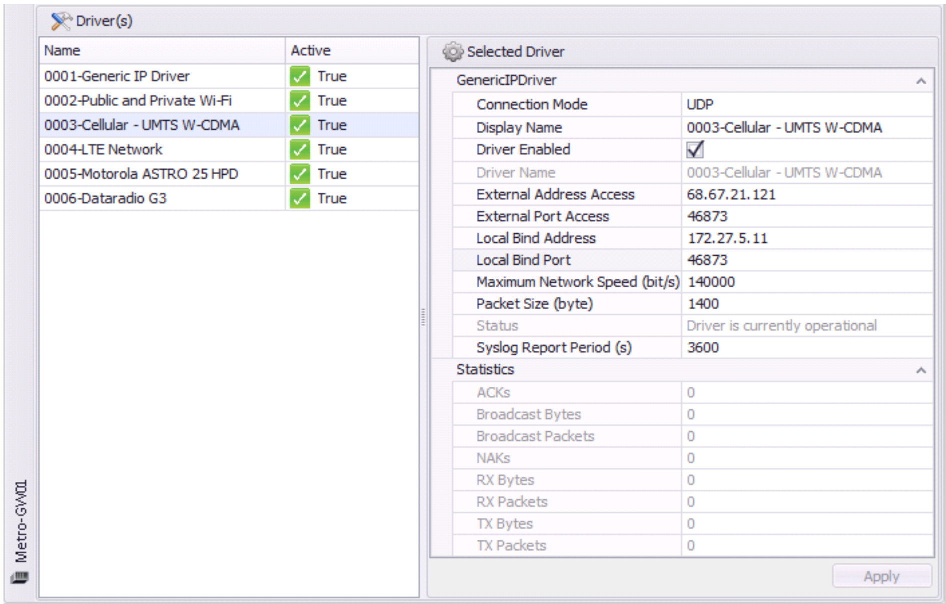
Once you are satisfied with the parameter values of your gateway communication driver(s), the next logical step is to configure client communication drivers into the system. Keep in mind that client communication driver settings are not visible until they populate functional groups as groups are created.

⚠ Take the time to configure as many communication drivers as you need in the near future, preferably before creating and populating functional groups. Especially true in the case of large-scale deployments, it is preferable to “fine tune” driver configurations at the gateway level than to have to review, set, change and apply settings at individual group level.

⚠ Gateway communication drivers are designed for system-wide use. However, any change made to driver parameters during routine operation will only take effect after successively applying the **Reload Policies** and **Publish Policies** at the level of each functional group.

⚠ If your mobile devices connect to cellular networks through dial-up (as opposed to an always-on connection), be sure to enable the “Allow other people to use this connection” feature of your RAS manager to support takeover by Mult-IP’s corresponding client communication driver.

Gateway Communication Driver Parameter Description



Name	Active
0001-Generic IP Driver	✓ True
0002-Public and Private Wi-Fi	✓ True
0003-Cellular - UMTS W-CDMA	✓ True
0004-LTE Network	✓ True
0005-Motorola ASTRO 25 HPD	✓ True
0006-Dataradio G3	✓ True

GenericIPDriver	
Connection Mode	UDP
Display Name	0003-Cellular - UMTS W-CDMA
Driver Enabled	☑
Driver Name	0003-Cellular - UMTS W-CDMA
External Address Access	68.67.21.121
External Port Access	46873
Local Bind Address	172.27.5.11
Local Bind Port	46873
Maximum Network Speed (bit/s)	140000
Packet Size (byte)	1400
Status	Driver is currently operational
Syslog Report Period (s)	3600
Statistics	
ACKs	0
Broadcast Bytes	0
Broadcast Packets	0
NAKs	0
RX Bytes	0
RX Packets	0
TX Bytes	0
TX Packets	0

Table 4: Generic IP Communication Driver Parameter Field Description - Gateway side

Field Name	Description
Connection Mode	Select UDP for fast transfer of non-critical data such as multimedia. Type TCP for data (such as text and web pages) requiring error correction and guaranteed delivery.
Display Name	You may change the default driver name for a more suitable driver name in your environment. This driver name is displayed on the client side, in the Mult-IP drivers deskband.
Driver Enabled	Click to toggle communication driver state between **Enabled** (green ✓ icon) and **Disabled** (red ⚠ icon), followed by **Apply** to confirm.
Driver Name	Display field identifying communication driver name as it appears in the Add Gateway Communication Driver wizard.
External Address Access	Type the public facing IP address used by clients to access each gateway. Note that this parameter does not propagate and must be set on each individual gateway in a load-balancing farm. This parameter is of particular interest to organizations running gateway in distinct geographical locations.
External Port Access	Type the public facing TCP or UDP port assigned to clients accessing the gateway on the selected communication driver. Port setting is secondary to the **External Address Access**. This parameter does not propagate and must be set on each individual gateway in a load-balancing farm. This parameter is of particular interest to organizations running gateway in distinct geographical locations. Note that while multiple communication drivers can share the same external address, each driver must be assigned its own port.
Local Bind Address	Type the IP address of the LAN interface used to bind load-balancing gateways**.** This task is optional but most IP-based environments should bind communication drivers to a single IP address.
Local Bind Port	Type the TCP or UDP port on the local interface (**Local Bind Address**) of the communication driver listening for incoming data from clients.

Field Name	Description
Maximum Network Speed (bit/s)	Represents the transfer speed in bits per second allowed on this network under normal circumstances. This setting throttles data output to the network to prevent data loss. Of course, if the network becomes busy because of dense traffic, data may be dropped and need to be retransmitted.
Packet Size (byte)	Maximum number of data bytes to pack into a single frame during transmission. This value is tied to wireless system performance: smaller packet sizes yield more reliable transmissions on narrowband private systems or in low signal strength conditions while larger packets yield better performance. An average value of 1400 bytes is appropriate for broadband drivers. Range 128..2048 bytes.
Status	Read-only indicator showing whether the communication driver is operational or not based on applied configuration. Possible values: “Driver is currently operational”, “Driver is currently disabled” and “Driver is currently not operational. Missing local bind IP, port already in use or local bind address is within MVPN range.”
SysLog Report Period (s)	Set gateway communication driver status monitoring interval (in seconds). Default is 3600 seconds. Monitoring interval may be set individually for each driver. Setting to a lower value increases reporting frequency, providing higher resolution, which may be desirable when monitoring a driver subject to frequent status changes.

Table 5: Motorola DataTAC Communication Driver Parameter Field Description - Gateway side

Field Name	Description
Activate Load-balancing	Enable for use in a Load-balancing environment. **Warning: Motorola DataTAC units can only operate in a load-balancing environment if an instance of Radio IP Mobility Manager 2.0 or later is actively managing Motorola RNCs.**
Broadcast System ID	Type the value (between 1 and 255) broadcast by Mobility Manager to inform the Motorola DataTAC devices on the status of individual Mult-IP Load-balancing Gateway availability.
CID	Type the Communication Host number (between 10 and 254) which identifies individual Mult-IP Gateways to the RNC. Refer to your RNC documentation for the range of supported values. Keep in mind that some cannot be replicated, as they are reserved for internal system use.
Display Name	You may change the default driver name for a more suitable driver name in your environment. This driver name is displayed on the client side, in the Mult-IP drivers deskband.
Driver Enabled	Click to toggle communication driver state between **Enabled** (green ✓ icon) and **Disabled** (red ⚠ icon), followed by **Apply** to confirm.
Driver Name	Display field identifying communication driver name as it appears in the Add Gateway Communication Driver wizard.
Gateway System ID	Type a number (between 1 and 254) which identifies a specific gateway In a Load-balancing environment. This number is used to associate a number of mobile devices to a specific Mult-IP Gateway. Used together with Radio IP Mobility Manager, the Gateway System ID eases management of multiple mobiles over a number of VRM / RNC links. In load-balancing mode, Mult-IP clients would automatically be forwarded to their associated hosts. The system may also be used to add extra system security because a Mult-IP Gateway will only accept connections from a client that has been set up with the same system number.
Group Call ID	Type the hexadecimal Group-call number. Defaults to EF4D4950. When specified, the Mult-IP / RNC system will be able to use the Group Call feature to target only those mobiles configured with the same Group Call number. Make sure not to change the default value. Group calls allow “broadcasts” type messages to be sent by server applications to only those VRMs that are used by a Mult-IP Client. VRMs will then avoid Group-call “broadcasts” that originate from irrelevant applications (such as CAD).

Field Name	Description
Missed Notifications Threshold	In a load-balancing environment, this value sets the number of broadcasts a mobile is allowed to miss before switching to another gateway.
Notification Period (s)	Sets broadcast frequency.
Operational State	Read-only indicator that the communication driver is online and supports data transfer based on applied configuration policy. Unchecked if one or many parameters are set in a way that prevents communication driver from operating at specified levels, such as erroneous port, Rnc IP address, packet size or speed.
Registration Session	Leave this field disabled. In some circumstances, this allows the Mult-IP Gateway to accept registration requests from clients.
RNC IP Address	Type the IP address assigned to the RNC.
Syslog Report Period (s)	Set gateway communication driver status reporting interval (in seconds). Default is 3600 seconds. Setting to a lower value increases reporting frequency, providing higher resolution, which may be desirable when monitoring a driver subject to frequent status changes.

Table 6: CalAmp Dataradio Communication Driver Parameter Field Description - Gateway side

Field Name	Description
ACK Carma (s)	Type the ACK delay (in seconds) allowed for packets originating from client modems.
Broadcast Address	Type the alphanumerical Dataradio address used by Mult-IP Gateways to issue messages to mobile modems**.**
Display Name	You may change the default driver name for a more suitable driver name in your environment. This driver name is displayed on the client side, in the Mult-IP drivers deskband.
Driver Enabled	Click to toggle communication driver state between **Enabled** (green ✓ icon) and **Disabled** (red ⚠ icon), followed by **Apply** to confirm.
Driver Name	Display field identifying communication driver name as it appears in the Add Gateway Communication Driver wizard.
ENQ Period (s)	Enter time delay (in seconds) for ENQ(uery) request for acknowledgement. If acknowledgement of the last packet has not been received in the delay defined by the Local ACK value, the system switches in ENQ mode and sends a request for acknowledgement at the end of each period specified in Local ACK.
Generate CRC	Check this box to add a CRC to the message for better transmission reliability. You may however disregard this setting since Packet Manager already adds its own CRC.
Heartbeat Period (s)	Enter the time (in seconds) between two heartbeats sent by a client to the gateway. Set to 0 to disable heartbeats.
Heartbeat Loss Threshold	Type the number of consecutive heartbeat packets (range: 1 to 25) sent by a client without gateway acknowledgement that will trigger a communication driver “disabled” or “out of coverage” condition. For example, a value of “3” implies that 3 consecutive client heartbeats sent without gateway acknowledgement will report driver as inoperable.
Local ACK (s)	Type the ACK delay (in seconds) from the local gateway modem.
Maximum Throughput (byte/s)	Maximum throughput allowed over the Dataradio network.
Maximum Number of Naks	Type the maximum number of negative aknowlegements allowed before declaring the mobile device out of coverage.
Naks Timeout (s)	Delay applied to packet acknowledgement.
Network Available	Leave to the default value (10000) to allow Dead Carrier Detection (DCD) over serial port connection. Set to “0” to defeat. Use of this feature requires the use of Gemini/PD G2 modems preloaded with firmware 16a.
Operational State	Read-only indicator that the communication driver is online and supports data transfer based on applied configuration policy. Unchecked if one or many parameters are set in a way that prevents communication driver from operating at specified levels, such as erroneous port, packet size or speed.
Packet Size (byte)	Maximum number of data bytes to pack into a single frame during transmission. This value is tied to wireless system performance: smaller packet sizes yield more reliable transmissions on narrowband private systems or in low signal strength conditions while larger packets yield better performance. An average value of 1400 bytes is appropriate for broadband drivers. Range 128..2048 bytes.
Read Period (mn)	Type the parameter refresh rate (in minutes).
RX Data (s)	Enter time (in seconds) allowed for complete reception of a message through the serial port.
Send Local Query	Check to enable the Dataradio local queries sending feature.
Systlog Report Period (s)	Gateway communication driver status reporting interval.
TCP Connection	Indicates the connection mode used (checked: IP, unchecked: Serial).
WACK Wait (s)	Type the wait delay (in seconds) after receiving a “WACK” before asking modem for transmit.

Table 7: Driver Statistics Field Description - Common to all drivers

Field Name	Description
ACKs	Number of acknowledgements for transmitted packets received by this gateway from the driver communication device.
Broadcast Bytes	Number of broadcast bytes sent by this gateway with this driver.
Broadcast Packets	Number of broadcast packets sent by this gateway with this driver.
NAKs	Number of negative acknowledgements for transmitted packets received by this gateway from the driver communication device.
RX Bytes	Bytes received on this gateway with this driver.
RX Packets	Packets received on this gateway with this driver.
TX Bytes	Bytes transmitted by this gateway with this driver.
TX Packets	Packets transmitted by this gateway with this driver.

Configuring Client Communication Drivers

To comply with the Mult-IP end-to-end communication mechanism, each communication driver added at the gateway requires a minimum of client-side configuration to account for such parameters as client hardware support, acceptable data throughput or data route management. See also the client communication driver parameter description table.

On some communication drivers, aligning gateway and client configurations may raise highly technical issues so make certain to have mobile hardware manufacturer documentation handy when performing this task. Some communication drivers however rely on basic parameters that are almost transparent at either end of the connection chain. Mult-IP provides for both situations by allowing users to perform client communication driver configuration using one of the following two approaches:

Running the Configure Client Driver wizard to create a client driver template:

1. Based on a fresh Mult-IP install, define one or several gateway communication drivers.
2. Right-click individual drivers and select **Configure Client Driver** from the context menu. Set applicable values.
3. Create one or several functional groups. Notice how each group inherits client driver properties.
4. Select **Publish Policies** to push new client driver configurations to individual mobile devices the next time they connect to the Mult-IP Gateway or as they are assigned to that functional group (See also: Processing New Client Connections).

Running the Configure Client Driver wizard to update Gateway driver properties:

1. In a production environment, edit one or several gateway communication driver properties to account for the latest corporate IP address assignments.
2. Right-click individual gateway drivers and select **Configure Client Driver** from the context menu. This time, do not change a single value, simply click **Next** until the wizard concludes.

3. Right-click individual functional groups and select **Reload Policies** to apply the latest gateway driver changes followed by **Publish Policies** to push new client driver configuration to mobile clients the next time they reconnect to the Mult-IP Gateway or as they are assigned to that functional group (See also: Processing New Client Connections on page 89). This simple approach applies to such communication drivers as Generic IP and Wi-Fi.

Note: The Configure Client Driver wizard features an editable field labeled **Local Bind Address**. Disregard this entry but DO NOT erase the supplied IP address.

Note: The Configure Client Driver wizard features an editable field labeled **Destination address**. Overtype existing value with the public facing IP address used by clients for connection purposes This IP address corresponds to the External Address Access.

Note: The Configure Client driver wizard applies only in those two instances described earlier. If, as part of routine system maintenance you wish to update parameters specific to individual functional groups, select a group and update field by overtyping existing value. Apply your changes(s) then select **Publish Policies** to push updated client driver configuration to mobile clients the next time they reconnect to the Mult-IP Gateway or as they are assigned to the updated functional group.

The following table describes parameters required for IP-type communication drivers. Those account for the vast majority of drivers currently supported by Mult-IP.

Table 8: IP Communication Driver Parameter Field Description - Client side

Field Name	Description
Driver Portlet	
Display Name	You may change the default driver name for a more suitable driver name in your environment. This driver name is displayed on the client side, in the Mult-IP drivers deskband.
Driver Enabled	Uncheck to disable driver. To enforce setting, publish new policies to gateway(s), then force a **Reset Connection** on clients of the selected functional group.
Driver Index	Read-only value assigned to each driver incremented with each newly installed driver. Use this value to identify driver in the roaming parameter string set for each pipe.
Driver Name	Display field identifying communication driver name as it appears in the Add Gateway Communication Driver wizard.

CalAmp Dataradio G2.	
ACK Carma (s)	Type the ACK delay (in seconds) allowed for packets originating from client modems (same as Gateway)
Baud Rate (bit/s)	Type the bits per second allowed on the selected serial port. Default is 19200 bauds.
ComPort	Communication port (such as COM1, COM2) in use by the radio modem connected to the mobile device.
Com Ports to scan	Commuinication ports to use for scanning ports (such as 1-5,6,7) to find radio modem connected to a mobile device. This option overwrites the ComPort option.
Data Bits	Type the size of the data bit to pack in a character frame.
Destination Address	Type the RF address of the corporate Dataradio server.
DTR/DSR	Check box if the radio modem makes use of the DTR and DSR pins.
ENQ Period (s)	Enter time delay (in seconds) for ENQ(uery) request for acknowledgement. If acknowledgement of the last packet has not been received in the delay defined by the Local ACK value, the system switches in ENQ mode and sends a request for acknowledgement at the end of each period specified in Local ACK.
GPS Local UDP Port	Open a local port on mobile device for reception of GPS coordinates. This port may then be used by applications such as Radio IP's GPS Partner to process raw GPS coordinates.
GPS Port	Leave to 5 (default). This value sets the internal Dataradio modem port used to transmit GPS coordinates.
Heartbeat Period (s)	Enter the time (in seconds) between two heartbeats sent by a client to the gateway. Set to 0 to disable heartbeats.
Heartbeat Loss Threshold	Type the number of consecutive heartbeat packets (range: 1 to 25) sent by a client without gateway acknowledgement that will trigger a communication driver "disabled" or "out of coverage" condition. For example, a value of "3" implies that 3 consecutive client heartbeats sent without gateway acknowledgement will report driver as inoperable.
Hunting Mode	Enable to allow mobile to connect to the first Dataradio base station to accept the connection request.
Local ACK (s)	Type the ACK delay (in seconds) for response from the local modem.
Maximum Number of Naks	Type the maximum number of negative aknowlegements allowed before declaring the mobile device out of coverage.
Maximum Throughput (byte/s)	Maximum throughput allowed over the Dataradio network.

CalAmp Dataradio G2.	
Naks Timeout (s)	Delay applied to packet acknowledgement.
Network Available	Leave to the default value (10000) to allow Dead Carrier Detection (DCD) over serial port connection. Set to “0” to defeat. Use of this feature requires the use of Gemini/PD G2 modems preloaded with firmware 16a.
Packet Size (byte)	Maximum number of data bytes to pack into a single frame during transmission. This value is tied to wireless system performance: smaller packet sizes yield more reliable transmissions on narrowband private systems or in low signal strength conditions while larger packets yield better performance. Range 128..2048 bytes.
Parity	Type the value of the parity bit. Leave to **None** (default) if no parity bit is used.
Read Period (mn)	Type the parameter refresh rate (in minutes).
RSSI Good (dB)	Set to a threshold value (in dB) at or above which Dataradio G2 radio modem enters “good” coverage conditions. Range -255..0.
RSSI Mode	Set to one of the following: “0” to defeat this parameter “1” to use “RSSI” only “2” to use “Signal Quality” only. “3” to use both “RSSI” and “Signal Quality” to assess “in-coverage” conditions.
RSSI Poor (dB)	Set to a threshold value (in dB) at or below which Dataradio G2 radio modem enters “poor” coverage conditions. Range -255..0.
RTS/CTS	Check to enable flow control indicator
RX Data (s)	Enter allowed time (in seconds) for full reception of a message through the serial port.
Send Local Query	Check to enable the Dataradio local queries sending feature.
Send Station Reset	Enable to allow mobile to connect to the first Dataradio base station to accept the connection request.
Signal Quality Good	Set to the threshold value (0-50000) at or above which Dataradio G2 radio modem is considered to be in good network quality conditions.
Signal Quality Poor	Set to the threshold value (0-50000) at or below which Dataradio G2 radio modem is considered to be in bad network quality conditions.
Stop Bits	Set the number of stop bits per character frame. Default set to **1** bit.
WACK Wait (s)	Type the wait delay (in seconds) after receiving a “WACK” before asking modem for transmit.
XON/XOFF	Enable to specify how software handles data transfer over the physical device. Match COM port settings to those provided by physical device specifications

G3 Plug-in Portlet – Use to implement Dataradio G3 out-of-coverage condition reporting for roaming purposes.	
Auto Detect Modem Address	Enable to allow the G3 plug-in to search among the available network interfaces, for a response on TCP port 6261. When used in conjunction with the "Enable roaming Status" option, it allows a roaming strategy without heartbeats.
Enable Roaming Status	Enable to allow the G3 plug-in to use Roaming Status information received from the G3 modem on TCP port 6261. Roaming Status information is used to enable a roaming strategy without heartbeats.
Gemini In Coverage Timeout (s)	Delay (between 5 and 30 seconds) allowed between the moment the modem first triggers a "Registering" condition and the moment the delay expires with no condition change, thus resulting in an "In-Coverage" condition.
Gemini Modem Address	This is the IP address used for the plug-in to receive roaming status information from the modem. Type the default gateway address assigned to the Gemini modem. Refer to product documentation or device label for actual values.
Gemini Out Of Coverage Timeout	Delay (between 10 and 60 seconds) allowed between the moment the modem first triggers an "Initializing" or "Roaming" condition and the moment the delay expires with no condition change, thus resulting in an "out-of-coverage" condition.
Gemini Status Port	TCP port reserved for communication with Gemini modem. Do no change this value.

General Portlet (generic IP driver)	
Connection Mode	Read-only indication of the Connection Mode driver configuration set on the gateway side. See Connection Mode.
Deskband Driver Type	Type the Mult-IP Client display attribute for on-the-fly identification of active communication drivers. Leave blank to displays the default radio modem icon Type **CELLULAR** to display cellular-based driver icon Type **SATELLITE** to display a dish-like icon Type **WIFI** to display a radio antenna-like icon Type **PRIVATERADIO** for PMR (private mobile network)-type driver icon
Heartbeat Period (s)	Enter the time (in seconds) between two heartbeats sent by a client to the gateway. Set to 0 to disable heartbeats. **Note**: If mobile devices are configured with Harris Opensky or Dataradio G3 drivers and you wish to rely on their internal RSSI in-range reporting feature, leave the Heartbeat Frequency to "0" (default) to overcome conflicts between the two in-range reporting options.
Heartbeat Loss Threshold	Type the number of consecutive heartbeat packets (range: 3 to 100) sent by a client without gateway acknowledgement that will trigger a communication driver "disabled" or "out of coverage" condition. For example, a value of "3" implies that 3 consecutive client heartbeats sent without gateway acknowledgement will report driver as inoperable.
Maximum Network Speed (bit/s)	Type the maximum speed permitted by the wireless network (in bits/sec.). Leave to "0" to allow speed to fluctuate with changing driver performance. Values between "1" and "14999999" will result in a max speed of 700 kbits/sec. A value of 15000000 will set max speed at 15 Mbits/sec. A value of "15000001" or higher will default speed to the the variable setting of "0".
Packet Size (byte)	Maximum number of data bytes to pack into a single frame during transmission. This value is tied to wireless system performance: smaller packet sizes yield more reliable transmissions on narrowband private systems or in low signal strength conditions while larger packets yield better performance. An average value of 1400 bytes is appropriate for broadband drivers. Range 128..2048 bytes.
Validate Gateway on UDP Reception	Enable so that clients validate that incoming packets as sent from a trusted gateway.

OpenSky Plugin Portlet	
Activate GPS	Enable to collect GPS information from OpenSky trunked radios supporting this feature. Keep in mind that you will need to properly set all associated client-side parameters as well.
Auto scan for COM ports	Using autoScanPort will scan serial ports to find your device.
Baud Rate (bit/s)	Type the bits per second allowed on the selected serial port.
ComPort	Type the communication port (such as COM1, COM2) in use by the radio modem connected to the mobile device.
Com Ports to scan	Commuinication ports to use for scanning ports (such as 1-5,6,7) to find radio modem connected to a mobile device. This option overwrites the ComPort option.
Data Bits	Type the size of the data bit to pack in a character frame. Default is **8 bits.**
Destination Address	Type the mandatory static LAN address of any Mult-IP Gateway in the same farm used to initiate client connection and registration.
Destination Port	Type the TCP port number (default is 46871) used to connect the client to the Mult-IP Gateway farm. Using UDP, data packets will be sent to this service port number.
DTR/DSR	Check box if the radio modem makes use of the DTR and DSR pins.
Escape Character	Character string (such as **) issued before invoking AT commands.
GPS Period (s)	Type a GPS data polling frequency. The default value of 1 sampling per second should be suitable for most application. Note that a higher value may yield higher accuracy, but may account for unwanted traffic on narrowband private networks
GPS Server Address	Type the LAN IP address of the computer hosting GPS routing software (such as Radio IP's GPS Director) or other GPS processing or CAD application.
GPS Server Port	Set to the LAN-based TCP listening port assigned to the GPS application.
Heartbeat Period (s)	Enter the time (in seconds) between two heartbeats sent by a client to the gateway. Set to 0 to disable heartbeats. **Note**: If mobile devices are configured with Harris Opensky or Dataradio G3 drivers and you wish to rely on their internal RSSI in-range reporting feature, leave the Heartbeat Frequency to "0" (default) to overcome conflicts between the two in-range reporting options.
Heartbeat Loss Threshold	Type the number of consecutive heartbeat packets (range: 3 to 100) sent by a client without gateway acknowledgement that will trigger a communication driver "disabled" or "out of coverage" condition. For example, a value of "3" implies that 3 consecutive client heartbeats sent without gateway acknowledgement will report driver as inoperable.
Initialization Retries	Maximum number of modem initialization attempts to perform before modem is reported as unavailable.
Initialization Timeout (s)	Time to wait for an answer from the modem (in seconds) before triggering an initialization error.
Medium Speed (bits/s)	Leave to the default value of 7200 bits/sec, which represents the transfer speed in bits per second allowed on this network under normal circumstances. This setting throttles data output to the network to prevent data loss. Of course, if the network becomes busy because of dense traffic, data may be dropped and need to be retransmitted.
Offline Character	OpenSky modem offline character (see escape charater above).
Online Timeout (s)	Maximum wait (in seconds) for connect timeout.
Packet Size (byte)	Maximum number of data bytes to pack into a single frame during transmission. This value is tied to wireless system performance: smaller packet sizes yield more reliable transmissions on narrowband private systems or in low signal strength conditions while larger packets yield better performance. Set to 512 (default) bytes to match Opensky packet size on the gateway side.
Parity	Type the parity bit in use. If none is used, leave default to **None**.
Protocol Version	Define which protocol to use to interface OpenSky modem. Possible values are Legacy, 2 and 3.
RTS/CTS	Check to enable flow control indicator.

OpenSky Plugin Portlet	
Stop Bits	Set the number of stop bits per character frame. Default set to **1** bit.
XON/OFF	Enable to specify how software handles data transfer over the physical device. In doing so, you will have to match **ComPort** settings to those provided by physical device manufacturer specs.

OpenSky Plugin Portlet, specifics for Dialup (PPP) device	
Heartbeat Loss Threshold	Type the number of consecutive heartbeat packets (range: 3 to 100) sent by a client without gateway acknowledgement that will trigger a communication driver "disabled" or "out of coverage" condition. For example, a value of "3" implies that 3 consecutive client heartbeats sent without gateway acknowledgement will report driver as inoperable.
Heartbeat Timeout (s)	Delay between two heartbeats in seconds. 0 means no heartbeat.
Validate Gateway On UDP Reception	Enable so that clients validate that incoming packets as sent from a trusted gateway.

OpenSky Plugin Portlet, specifics for SLIP device	
Auto scan for COM port	Using autoScanPort will scan serial ports to find your device
Heartbeat Loss Threshold	Threshold value that sets the number of heartbeats missed before the mobile device is declared out of coverage.
Heartbeat Period (s)	Enter the time (in seconds) between two heartbeats sent by a client to the gateway. Set to 0 to disable heartbeats.
Initialization Retries	Init command retries
Initialization Timeout (s)	Init command timout value
Online Timeout (s)	Online timeout value

PSCM (Public Safety Connection Manager) **Portlet**	
Modem Mode	Read-only field indicating if driver is in WiFi, BC13, PSST or EVDO mode.

Datatac Plugin Portlet	
Baud Rate (bit/s)	Bits per second allowed on the selected serial port.
Broadcast System ID	Broadcast system ID used to notify clients of gateway availability.
ComPort	Communication port (such as COM1, COM2) in use by the radio modem connected to the mobile device.
Com Ports to scan	Commuinication ports to use for scanning ports (such as 1-5,6,7) to find radio modem connected to a mobile device. This option overwrites the ComPort option.
Confirm Mode	Set/Clear confirm mode.
Data Bits	Size of the data bit to pack in a character frame. Default is 8 bits.
DTR/DSR	Check box if the radio modem makes use of the DTR and DSR pins.
Gateway System ID	Gateway System ID for Datatac Load-balancing.
Group Call ID	Group call ID in Hex format.
Load-balancing Enabled	Checked if Datatac Load-balancing Mode is enabled.
Missed Notifications Threshold	In a load-balancing environment, this value sets the number of broadcasts a mobile is allowed to miss before switching to another gateway.
Notification Period (s)	Sets broadcast frequency.
Packet Size (byte)	Maximum number of data bytes to pack into a single frame during transmission. This value is tied to wireless system performance: smaller packet sizes yield more reliable transmissions on narrowband private systems or in low signal strength conditions while larger packets yield better performance. An average value of 1400 bytes is appropriate for broadband drivers. Range 128..2048 bytes.
Parity	Type the parity bit in use. I none is used, leave default to **None**.
RTS/CTS	Check to enable flow control indicator.
Stop Bits	Set the number of stop bits per character frame. Default set to **1** bit.
XON/OFF	Enable to specify how software handles data transfer over the physical device. In doing so, you will have to match **COMPort** settings to those provided by physical device manufacturer specs.

RAS Plug-in Portlet	
Domain	Type the name of the network domain the user associated with the dialup profile belongs to (if applicable).
Password	Type the password associated with the dialup profile username.
RAS Connection Name	Type the dialup or VPN connection tied to the RAS account. Typical dialup configuration uses the Windows New Connection wizard to accessing the Internet or private networks.
User Name	Type the username (no spaces allowed) associated with the dialup profile.

Routing Portlet	
Additional Route 1	Use these two fields to set custom routes. Note however that subsequent removal of one or both routes will cause the client to reset driver.
Additional Route 2	
Interface Name	**Important**: Type the name of the connection configured in Windows that the driver will use for data transfer. This name will be mandatory if the **Use Configured Interface Only** option is enabled. See next.
Is Default Route	Check box to let Mult-IP add a route to the destination IP address for this driver. See External address access on page 44.
Need Default Gateway	Check box to force communication driver to wait for a default gateway supplied by the selected interface device on the mobile client. Failure to supply a default gateway prompts an error message.
Remove Interface Route	Check box in order to remove routes supplied for the selected interface.
Use Configured Interface Only	Check box to force the use of the selected interface. Uncheck to allow auto detection of an available interface. Do not uncheck if two or more interfaces are pointing to the same segment. Keep in mind that enabling this parameter will require that you provide an interface name before the **Apply** button can be used. See above. Note: To avoid situations where clients fail to send source IP to the gateway in a roaming situation, make sure to enable the **Use Confiugred Interface Only** option. Otherwise, the active driver will use whichever interface is available, even disregarding IP segment values.

SNMP Plug-in Portlet - Motorola Astro 25 HPD and IVD (IV&D) communication drivers feature handoff capability on poor RF quality when such notification is supported by the radio modem. To this end, Mult-IP requires that both SNMP and SNMP Trap Windows features are enabled on the mobile device in order to promptly respond to communication status changes.	
Check Modem Period (ms)	Actual modem polling period for SNMP check modem message (in milliseconds).
Enable In Range Trap	Check box to allow unsolicited events to report in-range status changes.
Enable RF Registration Status Trap	Check box to enable capture of HPD MSU’s RF Registration Statuses. Status value reporting as either “registered” or “registered and Site Locked” is added to RSSI and In-range modem polling (OID) to qualify mobile device “in range”. Failure to meet those three requirements flags the mobile as “out of range”.
Enable RSSI Trap	Check box to allow unsolicited events to report RSSI state changes.
In-Range Message OID	SNMP variable identifier used to poll modem variable indicative of in-range radio status. Note that modem response may not be interpreted as actual acknowledgement of in-range condition. Refer to RSSI for more accurate in-range condition reporting.
In-Range Value	Value indicative of in-range condition against which modem response is compared. This value is supplied by the radio equipment manufacturer.
Manager Register OID	This unique value allows modem registration to SNMP traps. This value should not be changed.
Modem Address	Type the unique default IP address value built-in your Motorola ASTRO® 25 IVD or HPD modem. Make certain to have two different addresses if two such modems are used on the same client workstation.
RF Registration Status Period (ms)	Set to HPD MSU’s RF registration status polling period (default 1000 milliseconds).
RF Registration Status OID	Set to one of the following: 1.3.6.1.4.1.161.3.6.30.2.2.1.3.7.0, or according to manufacturer instructions. This parameter sets the identifier sent to modem to query RF registration status.
RF Registration Status Value	Set to 2 (Registered), 3 (Registered and Site Locked) or both according to whether you want one or both values to be used in the “in-range” assessment algorithm triggered by the **RF Registration Status Trap** described above. **Note**: value separator can be space, comma, dot, dash or semicolon.
RSSI Period (ms)	Radio Signal polling period (in milliseconds).
RSSI Message OID	SNMP variable identifier sent to modem when querying RSSI.
RSSI Mode	Set to 0 for support of Radio IP’s legacy roaming algorithm. Set to 1 to support advanced algorithm which accounts for dBm readings.
RSSI Sampling	Set to the number of RSSI readings that, when added, average to a value equal or above the RSSI threshold for the purpose of reporting an “in-range” condition. This setting helps reduce quick back-and-forth roaming situations under rapidly changing signal conditions.
RSSI Threshold (dB)	Set to the minimum radio signal quality required for “in-range” status once added to the **In-Range value** set above.
SNMP Mode	Select **HPD** or **IVD** to match characteristics of the HPD or IV&D driver in use.
SNMP Request Timeout	Delay (in milliseconds) allowed before SNMP requests are ignored.

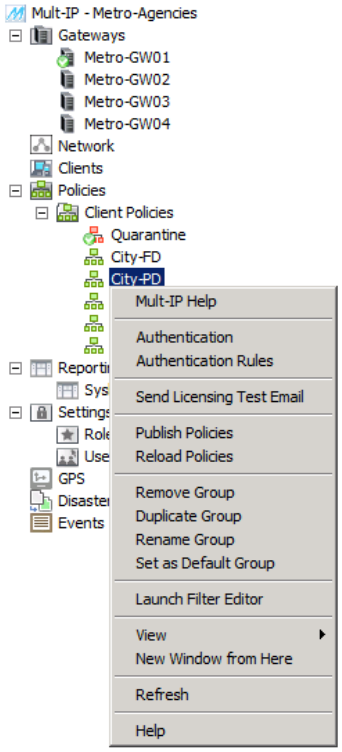
Policy Management

The Mult-IP Mobile VPN solution uses push technology to support mobile client policy updates with little to no downtime.

In their simplest form, policies can be viewed as sets of system settings designed to impact one or several groups of homogenous mobile clients. The process of pushing policies to clients takes two forms:

- Initially, a client connects and registers to an available gateway using default encryption and automatically joins the *Quarantine* group (if the default group has not been set to another group than Quarantine), pending operator acknowledgement. While browsing the client list, the operator acknowledges the new client by assigning it to a functional group.
- Alternately, a client may register and instead of being quarantined, it will automatically be redirected to a functional group set as default in which case the client will download and apply policies set for this group. Policies carry some or all of the following: communication driver payload, filter rules, roaming scenarios, authentication method and encryption. See also: Processing New Client Connections.
- While performing routine fleet management, the operator may occasionally publish new policies to one or several functional groups for such purposes as implementing (or switching) authentication, adding communication drivers or changing pipe assignments via filter rules. Updated policies take effect as new clients are assigned to the target group or as existing client connections are reset.
- Policies are not designed to be published to all clients in one “sweep”. They are designed at the group level and intended for clients of that group, offering a justification for the number of groups you wish to maintain. On one hand, if fleet size and logical distribution is not a concern, you may simplify fleet management by creating a single group, set it as default and define policies that will be applied to all clients. On the other hand, if your fleet involves multiple agencies operating in distinct geographical locations, you will have to support multiple groups and design/apply policies that will account for group characteristics, even though the entire fleet of mobile clients may share the same communication driver settings.

Even though some parameters (such as encryption) are system-wide, all Mult-IP parameters are part of policies managed at the functional group level. To help illustrate the principles of policy management, let’s recall the five-agency organizational structure introduced earlier.



Principles of Policy Management

A newly installed Mult-IP Client supports direct connection to a Mult-IP Gateway using wired LAN or local WI-FI secured by triple-DES encryption. This minimal configuration should prove sufficient for most mobile workstations and will allow secure connection and registration to the gateway for receiving further configuration payload (policies).

The Mult-IP system was designed to provide a seamless client user experience by implementing policies as the preferred method through which changes are applied to client settings. In other words, any change in configuration to any area of the Mult-IP system with the potential to affect any client in the fleet will require a policy update at the very minimum. What follows is a point-by-point description of the publishing mechanism and how it is designed to behave at different levels of the system hierarchy.

- **Applying a change to the entire fleet** – following the setup of a new public firewall, you may need to update External IPs and ports for each Mult-IP’s Ip drivers. To achieve this, for each driver you need to change the settings in the driver configuration pane on the gateway side, then Reload Policies to grab any top-level configuration change, then apply Publish Policies to save changes in the gateways.
- **Limiting the scope of a policy change** - new corporate directives may require that you switch a group of clients from an EVDO/CDMA to a 3G/GSM cellular carrier. In the Mult-IP environment, this calls for new communication driver definitions pushed to clients. To do this:

1. Add and configure the newly used driver on a gateway. It is automatically propagated to each gateway within the context.
2. Right-click a group, such as *Police Dept*, and select **Reload Policies**. This first of two steps applies new settings to the group's current policy definition. While this step has the ability to overwrite key areas of your client communication driver definition such as Connection Mode (UDP/TCP), rest assured that custom values will persist.
3. Enable the new added driver to be effective in this group. If you have more than 8 drivers, open the Concurrent Network Tab and add the driver ID in the "Driver Roaming Priority" list.
4. Select **Publish Policies** to save settings in the system. The policy update will be downloaded to clients of the *Police Dept* group as they reconnect to a Mult-IP Gateway (following a Reset Connection). Note that clients assigned to other groups are not affected by the target group's policy update.

- **Applying policies to a single client** - Despite the fact that the management console cannot show individual clients in the system hierarchy, polices can be managed at a granular level and as such, imposes no limit on the number of individually managed clients for such purposes as test or guest access. To do so:

1. Create as many single-client "special purpose" group containers as you need, each one clearly identifying their individual target client, such as **Guest User** or **John Smith**. In doing so, the latest system configuration template is copied onto the newly created groups.
2. Review client communication driver definition, concurrent networking and other features you want to apply to this client. Then select **Publish Policies** to save settings in the system configuration file.
3. Allow a client to register to the default group, then assign to a special-purpose group. In doing so, the client will automatically apply the policies attached to that group. As always, the client will download and apply policies upon re-registration and such payload will remain valid for as long as the client is not moved to another group.

Adding functional groups

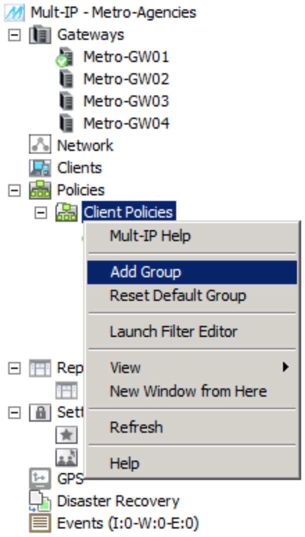
A functional group node can be defined as a collection of clients sharing common attributes in order to facilitate fleet management and policy updates. One basic rule to keep in mind when considering group creation is that once deployment takes effect, all members of a given group inherit and apply the same policy payload which contain, but is not limited to:

- Communication driver interface settings
- Concurrent network usage
- Authentication method (Windows, Radius, 802.1x)
- DHCP leasing, Split tunneling, etc.

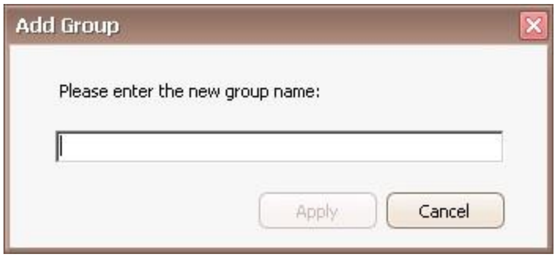
To minimize burden, functional group should only be created once all gateway communication drivers have been added and client communication drivers configured. Recall that this first step takes into account all public and private wireless systems that could potentially be used by any user in the foreseeable future. Meeting this requirement ensures consistency between the number of drivers defined at the gateway level and those available to any client group.

Each functional group inherits the complete list of gateway communication drivers at the time of creation. Then it is up to the system integrator to customize client communication drivers to the hardware specs or field conditions of the clients in that group.

To add a functional group,



1. As shown, browse the system tree, and expand the **Policies** node and right-click **Client Policies**.
2. Select **Add Group** from the context menu to bring up the Group Name box.

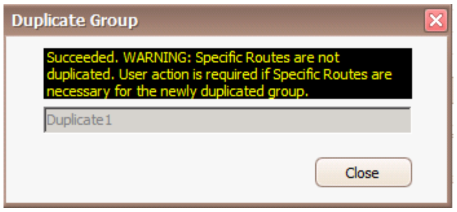


3. Type a meaningful name for the new functional group of maximum length 40 characters. Group names are handling is not case-sensitive, spaces are supported but special characters ! * & ‘ < > \ / “ are prohibited.
4. Click **Apply** to add the group to the Mult-IP system tree.

At this point, you may click on the newly created functional group and start customizing features such as client communication driver settings, concurrent network usage, authentication, and so on.

To speed up the creation of functional group you may use the “Duplicate Group” action located on the actions pane to replicate the configuration of an existing group to a new one.

Note: When duplicating a group, some of the original Specific Routes might not be copied. Therefore, you need to check the routes in the newly created group and add manually the missing ones to complete the duplication. The following message will be displayed as a reminder:



Duplicate Group

Succeeded. WARNING: Specific Routes are not duplicated. User action is required if Specific Routes are necessary for the newly duplicated group.

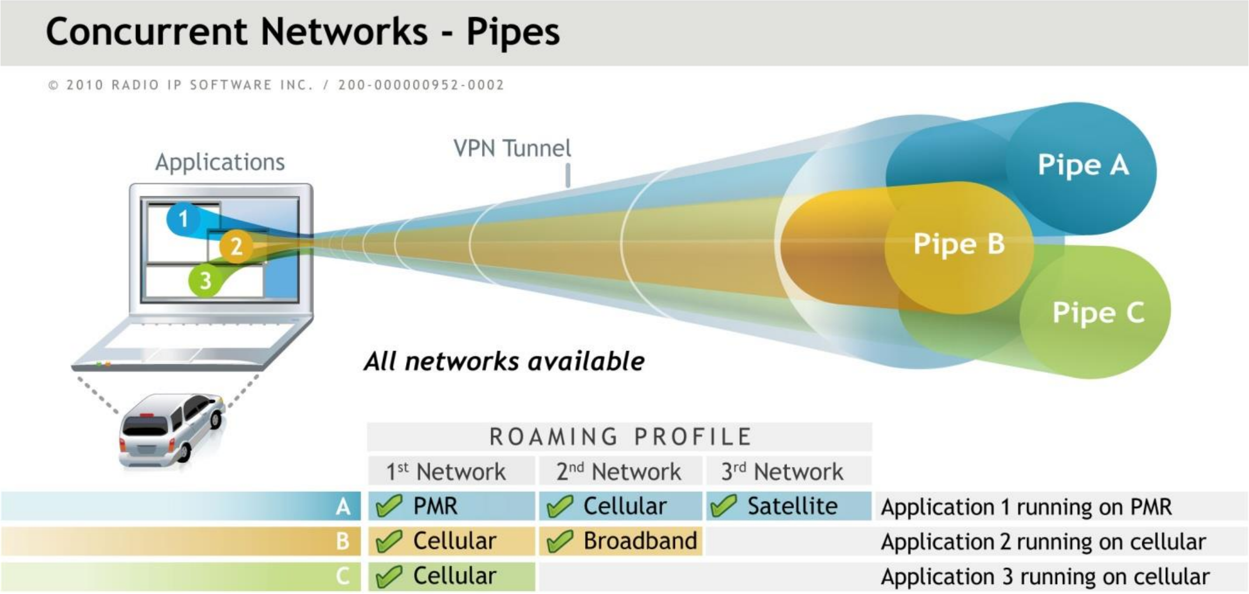
Duplicate1

Managing Concurrent Networks

This first of two sections discusses the Packet Manager toolbox used to manage the way data packets are handled between gateways and clients. It shows you how to plan communication drivers for use with specific types of data packets and to channel them to one of eight user-configurable pipes, resulting in groups of mobile clients capable of processing concurrent networks. This task relies on the following assumptions:

- You have already added all the gateway communication drivers that you plan to use in the foreseeable future.
- You have good understanding of corporate network data usage to the point where you can envision how mission-critical data (such as CAD, video or voice) should be prioritized over less-timely applications such as emailing or internet browsing.

From a technical standpoint, each Mult-IP functional group supports up to eight concurrent data pipes in the course of one VPN session. The system administrator begins by associating a pipe to different communication drivers in order of priority to form a roaming profile. Later on, specific application data can be matched to a specific pipe (see Controlling Traffic) ensuring that data will be carried on the most suitable or best performing network(s) with respect to narrowband and broadband usage.



Concurrent Networks - Pipes

© 2010 RADIO IP SOFTWARE INC. / 200-000000952-0002

	ROAMING PROFILE			
	1st Network	2nd Network	3rd Network	
A	✓ PMR	✓ Cellular	✓ Satellite	Application 1 running on PMR
B	✓ Cellular	✓ Broadband		Application 2 running on cellular
C	✓ Cellular			Application 3 running on cellular

***Figure 2**: Matching pipes and communication drivers to form a roaming profile*

For example, a pipe can be associated with a PMR (Private Mobile Radio) network as the primary network and a cellular network as secondary, while a second pipe can prioritize WI-FI with broadband cellular as secondary. A CAD application can be mapped to the first pipe while a video streaming application uses the second pipe. During a given VPN session, the dispatch data is carried over the PMR network and video streaming simultaneously travels over cellular, hence concurrent network usage. At any point, the client would switch to a known Wi-Fi network should one become available in order to cut costs and maintain video streaming in a seamless user experience.

Configuring Packet Manager

Packet Manager parameters are contained in the **Concurrent Networks** tab for each functional group and are unique to each pipe. They allow you to tune throughput performance to the sum of all gateway communication drivers associated with the pipe being configured. Keep in mind that Packet Manager should only be accessed by advanced radio system professionals with the knowledge to leverage performance between public broadband and private narrowband networks.

Note: The settings suggested in this section greatly impact Mult-IP behavior as well as over-the-air data flow. Packet Manager settings will greatly benefit from a good understanding of the radio coverage and data transmission profile.

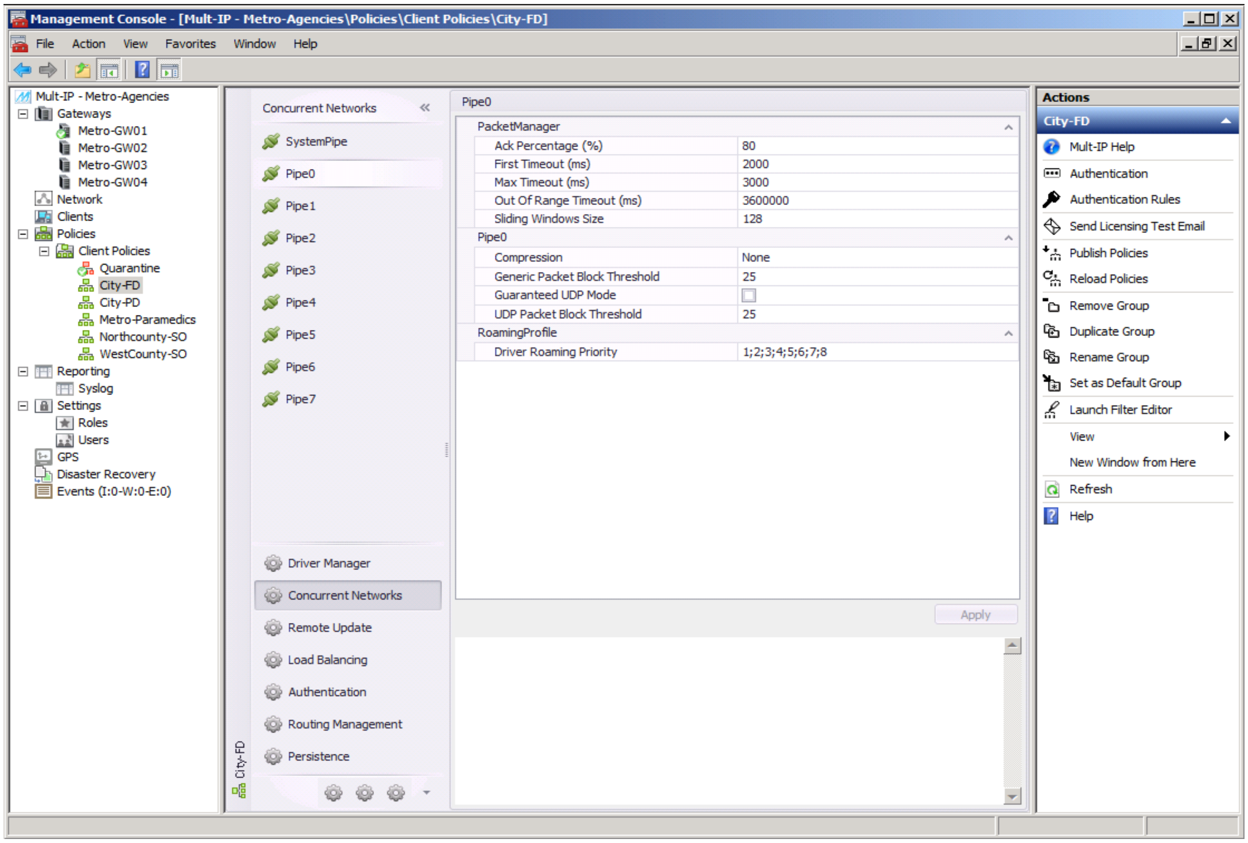
Before accessing Packet Manager parameters, familiarize yourself with the following pipe restrictions:

- **SystemPipe** (System Pipe) - comes preconfigured for use during mobile client registration. It suggests a default roaming profile of 1;2;3;4;5;6;7;8 where 1 represents the communication driver index for the built-in IP driver. This sequence is valid for up to 8 drivers, in which 7 are user-added drivers with a driver index incremented as communication drivers are added. While you may rearrange the driver index sequence to put the most reliable network first, to maintain a viable registration channel, make sure to that a driver is not deleted accidentally at startup of the mobile client or whenever users are required to perform a **Reset Connection** or **Restore Factory Defaults** on the mobile client.
- **Pipe0** – By default, Pipe0 is used by non-filtered traffic. This is a built-in assignment, which provides a path for packets that are not redirected to other pipes through the application of filter rules.You can change the default pipe using the filter rules.
- **Pipe1, Pipe2, Pipe3…, Pipe7** - user configurable pipes for the purpose of characterizing data packets according to the type of application they are targeting. Use those seven pipes to match data usage to the needs of demanding field applications. Once your functional needs are defined, you may begin by fine tuning the **Packet Manager** section keeping in mind the average performance expected from the least performing communication driver listed in your roaming scenarios. For example, if one wishes to assign **Pipe3** to mission-critical voice packets, care must be given to characteristics such as low timeouts, low latency, network reliability, and so on.

Note: Remote update traffic is channeled to **Pipe3**. Therefore, when defining a roaming profile for **Pipe3**, you are encouraged to prioritize broadband communication drivers in order to optimize support for the update process when in range of broadband networks.

To configure a Packet Manager,

1. Select the group you want to configure for concurrent networking, then click the **Concurrent Networks** tab in the selected group workspace.



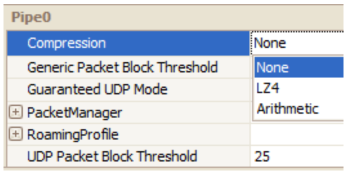
Pipe0

PacketManager	
Ack Percentage (%)	80
First Timeout (ms)	2000
Max Timeout (ms)	3000
Out Of Range Timeout (ms)	3600000
Sliding Windows Size	128
Pipe0	
Compression	None
Generic Packet Block Threshold	25
Guaranteed UDP Mode	□
UDP Packet Block Threshold	25
RoamingProfile	
Driver Roaming Priority	1;2;3;4;5;6;7;8

2. Select **SystemPipe** or one of eight user-configurable pipes and configure **Driver Roaming Priority parameter** as per field description provided in the next table.

Note: To support client registration in challenging field conditions, review **SystemPipe Packet Manager** settings so that they match the performance requirements of your narrowband wireless network(s).

Note: **Compression** field in the **Pipe** section allows two types of compression: LZ4 and arithmetic, giving flexibility on how you can increase your traffic throughput. As you can define the compression type for each pipe, it is recommended to select the arithmetic option on slow networks (better compression rate) and LZ4 otherwise (better computing efficiency):



Pipe0

Compression	None
Generic Packet Block Threshold	
Guaranteed UDP Mode	
⊞ PacketManager	
⊞ RoamingProfile	
UDP Packet Block Threshold	25

If you are using UDP-based application, it is necessary to select the **Guaranteed UDP Mode** pipe option for compression to work properly.

3. Review your settings and click **Apply** to register.

4. Click **Publish Policies** in the Actions pane to save your settings in the system. The new Packet Manager configuration policy is now available to mobile clients newly assigned to this group and to existing group clients the next time they reconnect to a gateway.

Table 9 : Pipe Configuration Field Description

Field header	Description
PacketManager Portlet	
Ack Percentage (%)	Packet Manager is designed to send an Ack after a given number of packets have been successfully sent. The number of packets is a percentage of the value specified in the sliding windows size. Therefore, a default windows size of 128 and an ACK Percent of 80 implies that Packet Manager will send an ACK packet after 102 successful packets are sent. Range: 1 to 100.
First Timeout (ms)	Timeout (in milliseconds in the range of 1 to 60000) beyond which an Ack packet is expected. Values range from a minimum of ~ 200 ms for broadband or a maximum of ~ 5000 ms for narrowband networks.
Max Timeout (ms)	Maximum timeout (in millisecond) value reached by the Ack packet request algorithm. If the **First Timeout** for an Ack reception is elapsed without an Ack reception, Packet Manager will request again an Ack packet from the destination with increasing delay up to the Maximum Timeout value is reached, then the period for an Ack request is set to the Maximum Timeout value until an Ack packet is received. Range: 1 to 60000.
Out of Range Timeout (ms)	Amount of time (in milliseconds) before the pipe is considered non-responsive due to a lack of response to an ACK packet.
Sliding Window Size	Displays the maximum size (number of packets in the range of 1 to 65535) of the IP buffers that can be sent. Packets in excess of this buffer size will be rejected but the sending network device will keep retrying to send them. They will be accepted once the space of the window size returns below its maximum size. For use with the **UDP Packet Block Threshold**. For instance, 10 connections set to a **UDP Packet Block Threshold** of 25 amount to 250 packets. A **Sliding Window** size of 128 implies that 128 packets of the original 250 packets will be accepted by the Packet Manager for the current pipe, Excess packets will remain in their respective buffer until Packet Manager sends packets to their destination. The buffering mechanism equally applies to both ends of the connection chain.
Pipe Portlet	
Compression	Select the type of compression applied on TCP/UDP packets on the selected pipe. For instance, you may decide to disable compression if the pipe being configured uses broadband communication drivers only. However, you may prefer to enable compression if you are anticipating traffic such as FTP or video streaming. Use preferably arithmetic compression on slow networks and LZ4 otherwise. Note that compression cannot be applied on the System Pipe.
Generic Packet Block Threshold	Set to the maximum number of TCP packets buffered before requesting an ACK from the other end. Excess packets will be dropped until all buffered packets have been sent and acknowledged by the computer at the receiving end.
Guaranteed UDP Mode	Check box if you want your UDP application data to be controlled and managed by the Mult-IP Packet Manager (i.e. allow retries if a packet is lost). Otherwise, UDP data is sent without any control mechanism.
UDP Packet Block Threshold	Set to the maximum number of UDP packets buffered before requesting an ACK from the other end. Excess packets will be dropped until all buffered packets have been sent and acknowledged by the computer at the receiving end.

Field header	Description
Roaming Profile Portlet	
Driver Roaming Priority	Use to build the actual roaming profile. Enter a driver index for each wireless network you wish to associate with this pipe for roaming purposes, in decreasing order of priority. Use the default sequence as a template and replace (overtype) each digit with custom values. As shown, digits must be separated by semi-colons (;) without spaces. **Note**: The **Driver Roaming Priority** is required by design. The console will therefore generate a non-fatal anonymous error message should the field be left empty. However, failure to provide adequate numerical values (matching drivers indexes) will prevent client registration to a gateway.

Quality of Service (QoS) Support

Mult-IP's streamlined TCP/IP packet header supports Quality of Service (QoS) by containing a TOS (Type of Service) field that encapsulates QoS information of the original IP header in both upstream and downstream communication. Recall that one of the building blocks of the Mult-IP TCP-IP mechanism is the ability to remove unnecessary overhead from original IP packet headers to conserve the much needed bandwidth over private or public narrowband networks.

While this is not mandatory, implementing QoS metrics at the corporate level offers the advantage of improved bandwidth reservation and delivery guarantee by prioritizing application traffic.

On Windows workstations (Vista and later) and Windows Server 2008, IT administrators can associate a QoS value to application from domain group policies, so existing or legacy application can benefit from the QoS mechanism without modification. OSs as well as network routers and switches can use QoS data to prioritize bandwidth on the basis of QoS values and rules set up by network administrators.

When applying QoS to packets in transit through Mult-IP, be aware of the following considerations to avoid pipe congestion and the dreaded degradation of critical application performance.

- Before transmission can take place, application-specific IP packets are encrypted into a secured packet whereas multiple source packets can "fit" into the resulting transmitted packet and with it, multiple QoS values may coexist.
- Relying on QoS rules (adding QoS values to the data) may cause pipes to fill and enter a waiting state if mismanaged. Keep in mind that a finite number of packets can be in transit at any given time and if they consist in many low priority packets mixed with a few high priority packets, the pipes would eventually be filled with the lower priority packets waiting to complete transmission, leading to pipe congestion and performance degradation.
- Mult-IP prevents pipe congestion by ensuring that data sent to a pipe is eventually transmitted by a communication driver. For IP networks such as LTE, data transits over an IP network that supports QoS rules. Packets sent from a pipe to the other end will carry the same QoS value that the last packet sent to the other side but not yet acknowledged. This implies that packet A with a QoS of 34 has been sent but not yet acknowledged, then new packet B with a QoS value of 0 will be set to 34 when sent. In this case, lower priority packets will be automatically "promoted" to a higher priority because they are transmitted on the same pipe as high priority data.
- Preventing pipe congestion can have adverse effects if disparate QoS data is sent on the same pipe, potentially causing low priority data to become high priority data. To mitigate this risk, apply filter rules to route data of comparable priority on the same pipe. For example, let's consider a 4-level QoS prioritization:
  - QoS 50-59 -> critical
  - QoS 40-49 -> High

- QoS 30-39 -> Medium
- QoS 0-29 -> Low

Then these applications should be grouped together on pipes 0 to 3. This way, low priority data such as web browsing will not automatically be promoted to critical data, which could interfere with critical applications.

Controlling Traffic

Traffic control is the final building block in your Mult-IP Concurrent VPN solution. It acts as a gatekeeper mechanism to control how application data is handled across the eight pipes provided for each functional group. The general goal is to channel demanding application packets to pipes with the highest performance, matched with broadband networks. This allows system integrators to optimize usability of narrowband PMR (Private Mobile Network) by isolating it from traffic generated by broadband data.

Traffic generated by a client can be addressed by way of the following:

- The target IP address and port;
- Pipe performance with respect to wireless network(s) associated with it.

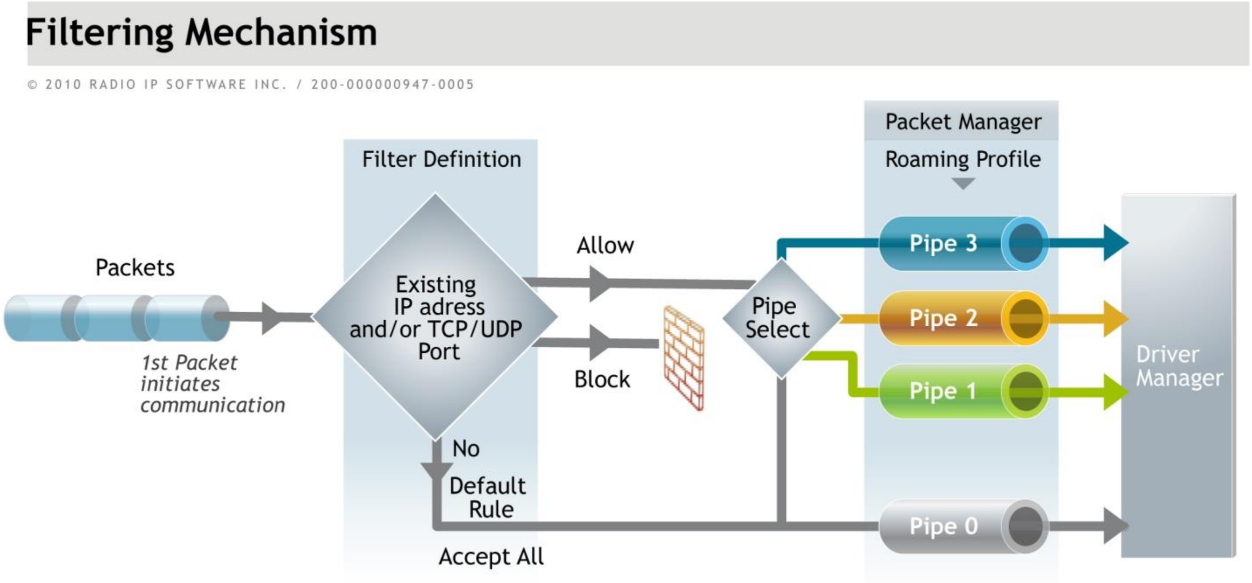


***Figure 3**: Filtered packet flow outlining how filter rules are used to target one default pipe among eight -purpose pipes.*

Figure 3 illustrates managed traffic control using a set of rules applied to all incoming connections. Once a valid connection to the gateway is established, client application packets are monitored by the filter module for their ability to meet certain conditions characterized by:

- **IP address** (pointing to an application server, public www address, and so on)
- **Port number** (TCP or UDP port assigned to a specific application)

Each rule consists in a set of conditions designed to target one of eight pipes when met. There is no limit to the number of rule/pipe combinations, but a handful should suffice in most situations, with each rule using some of the above information as input. Filter evaluation is triggered by the topmost rule in the list, with connection packet compared to rule constant; if it matches conditions, an answer of type *Accept* or *Block* is issued, and rule evaluation stops. If the first rule does not apply, then the second one is evaluated, then the third, and so on, until a rule applies and provides an answer. The “default” rule, illustrated in Figure 3 as a global *Accept all* rule, will ultimately apply if the bottom of the list is reached.

Note: Keep in mind that even though all eight pipes are user-customizable, Mult-IP comes preconfigured with a default rule set to accept all packets on **Pipe0**. Even though this is not mandatory, you are encouraged to define a set of rules that accounts for this default rule. When you define your rule set, it is suggested that you use Accept-type rules to allow specific pathways, and to terminate your rule set with a Block All.

Note: Remote update traffic is channeled to **Pipe3** and that assignment cannot be changed. Remember this constraint when defining rules that route specific types of packets to Pipe3 so as preserve the efficiency of the remote update process.

As indicated earlier, filter rule sets are specific to each functional group. They are first defined then saved as policies applied by new clients assigned to the functional group or by existing clients when they reconnect to a Mult-IP Gateway. A verification process ensures that rules are sent to clients only if their current set is different from what is found on the gateway.

Here are a few examples of what rules may be used for:

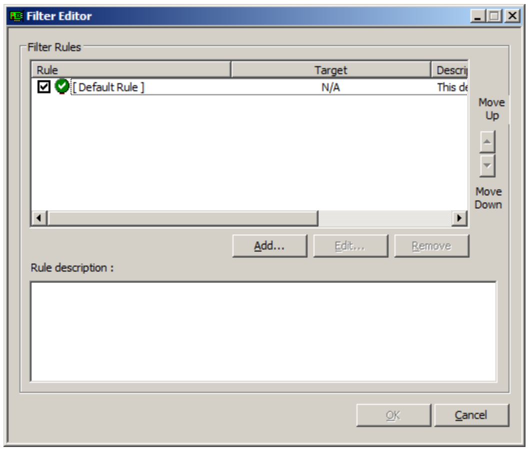
- you may allow mobile workstation applications to be updated over a Wi-Fi network only;
- you may disallow mapping software updates on a private, narrowband, network;
- you may decide to deny a slower network access to a particular server;
- you may allow report management software to always use the fastest network installed.

Managing Rules

The next set of instructions provides an overview of the filtering mechanism. Read on to learn how to launch the Filter Editor wizard, edit the default rule and create rules for custom packet filtering.

To launch Filter Editor,

From the management console's system tree, select the functional group whose traffic you want to manage and click **Launch Filter Editor** from the Actions pane to display the filter interface window shown next.

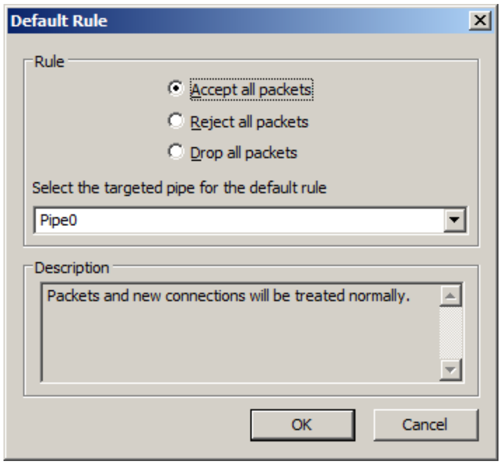


Rule	Target	Descri
☑ ✓ [Default Rule]	N/A	This de

Note: The default rule cannot be removed. However, it can be edited to meet corporate requirements.

To edit the default rule,

1. Select **Default Rule** from the main filter editor interface, then click **Edit**.
2. Set Default Rule window parameters as described next.


Default Rule
Rule
● Accept all packets
○ Reject all packets
○ Drop all packets
Select the targeted pipe for the default rule
Pipe0
Description
Packets and new connections will be treated normally.
OK
Cancel

a) **Accept all packets**: All TCP and UDP traffic are allowed through the selected pipe.

b) **Reject all packets**: A TCP connection is intercepted and a reset is sent preventing it from establishing. In doing so, requests from the source application are rejected allowing the application to process the error immediately, providing some feedback to the user.

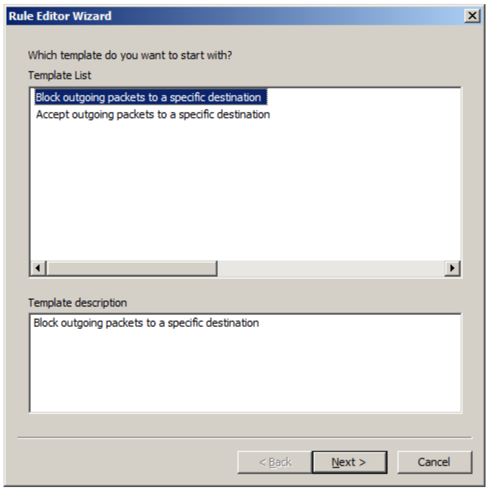
c) **Drop all packets**: Packets are not processed. TCP and UDP connection requests are discarded and the application (such as browser or mail client) simply times out. If a connection is attempted, no notification is sent to break or stop the connection (stealth mode).

Note: UDP packets cannot be rejected: they can either be accepted or dropped.

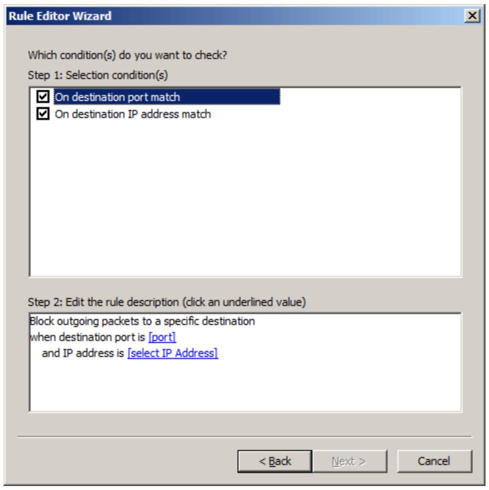
To create a rule for the purpose of blocking outgoing packets to a specific destination or port,

This rule intercepts packets targeting LAN assets (such as an application listening on a specific port).

1. Return to the Filter Editor main interface and click **Add**. This will allow you to create a custom rule designed to block outgoing packets to a specific destination.


Rule Editor Wizard
Which template do you want to start with?
Template List
Block outgoing packets to a specific destination
Accept outgoing packets to a specific destination
Template description
Block outgoing packets to a specific destination
< Back
Next >
Cancel

2. Select the template that matches the desired action on outgoing client packets from the Template List and click **Next**.
3. Add one or both conditions to the new rule. A criterion selector appears in the lower pane to complete configuration of the selected condition.



Rule Editor Wizard

Which condition(s) do you want to check?

Step 1: Selection condition(s)

☑ On destination port match
☑ On destination IP address match

Step 2: Edit the rule description (click an underlined value)

Block outgoing packets to a specific destination
when destination port is [port]
and IP address is [select IP Address]

4. For every condition that you have selected above, determine the criterion more precisely. Click the **[port]** and **[select IP Address]** successively to set their detail.

Refer to the following subsections for more information.

To select ports,

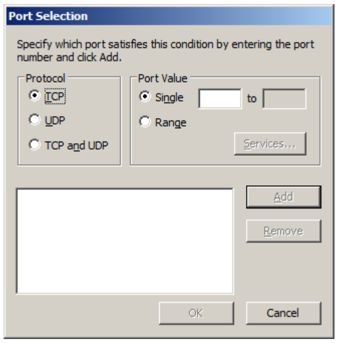
a) Under **Protocol**, select the protocol to which the rule will apply. You may also click **TCP and UDP** to encompass both.

b) In the **Port Value** section, define whether the rule will apply to a single port, or to a port range (including limits).

c) Click **Add** once you have set protocol and port. Note that you may add as many port settings as your application requires.

d) Select port criterion from the list and click **Remove** if you wish to discard and start again using different values

d) Click **OK** to register the criterion.



Port Selection

Specify which port satisfies this condition by entering the port number and click Add.

Protocol: ● TCP ○ UDP ○ TCP and UDP

Port Value: ● Single ○ Range; to

To select an IP address,

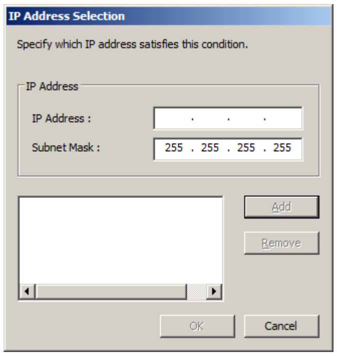
a) Enter the IP address the rule should apply to in the **IP Address** section.

b) Make sure **Subnet Mask** displays 255.255.255.255.

c) For each IP address that you define this way, click **Add** to enter into the rule.

d) Select IP criterion from the list and click **Remove** if you wish to discard and start again using different values

e) Click **OK** to accept.



IP Address Selection

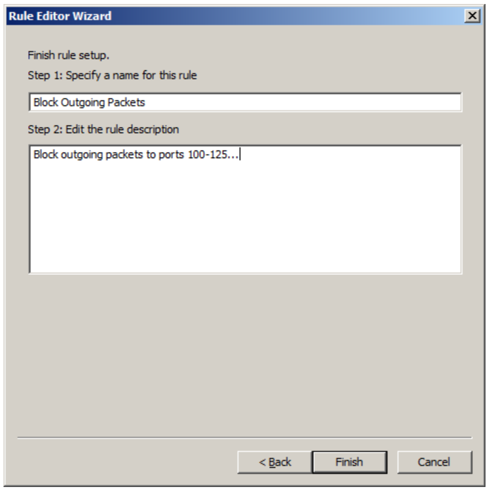
Specify which IP address satisfies this condition.

IP Address

IP Address : . . .

Subnet Mask : 255 . 255 . 255 . 255

5. Back to the Rule Editor Wizard, click **Next** once conditions are set.
6. Enter a name and a description for the rule.



Finish rule setup.

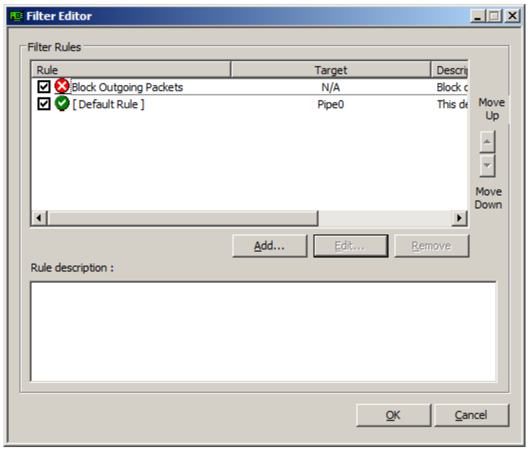
Step 1: Specify a name for this rule

Block Outgoing Packets

Step 2: Edit the rule description

Block outgoing packets to ports 100-125...

7. Click **Finish** to add the rule to the list. As shown next, make sure the new rule is checked in order to make use of it.



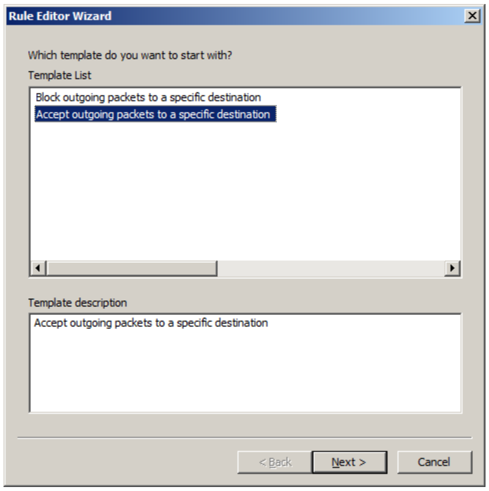
Rule	Target	Descri
☑ Block Outgoing Packets	N/A	Block c
☑ [Default Rule]	Pipe0	This de

8. Optionally, you may select a rule and review its description in the lower pane.
9. Click **OK** to save the rules and close Filter Editor.
10. Right-click the functional group targeted by the newly defined filter rule(s) and click **Publish Policies**. The rules will be saved in the system and applied to new mobile clients assigned to this group and to existing group clients as they reconnect to a Mult-IP Gateway.

To create a rule designed to accept and route packets to a specific pipe,

Note: Rules are defined to accept packets on a given pipe or to block packets on all pipes. Assign any accept-type rule to **Pipe1** through **Pipe7** to isolate specific packets or otherwise "relieve" **Pipe0**.

1. Return to the Filter Editor main interface and click **Add**. This will allow you to create a custom rule designed to accept outgoing packets to a specific destination.



Which template do you want to start with?

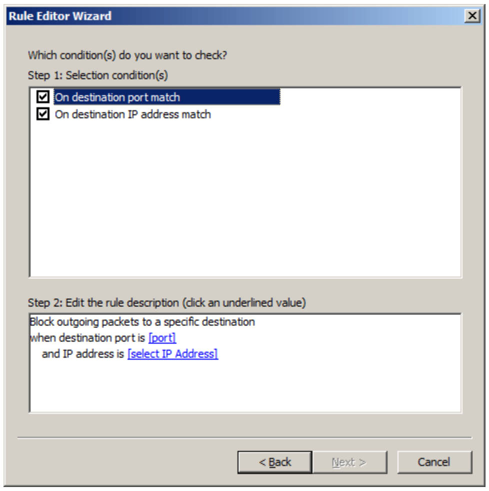
Template List

Block outgoing packets to a specific destination
Accept outgoing packets to a specific destination

Template description

Accept outgoing packets to a specific destination

2. As shown, select the **Accept all outgoing packets…** template and click **Next**.
3. Select the desired conditions. A related criterion selector appears in the lower pane.



Which condition(s) do you want to check?

Step 1: Selection condition(s)

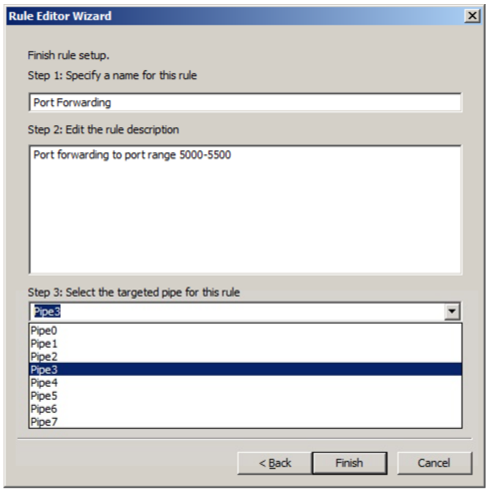
☑ On destination port match
☑ On destination IP address match

Step 2: Edit the rule description (click an underlined value)

Block outgoing packets to a specific destination
when destination port is [port]
and IP address is [select IP Address]

4. For every condition selected above, determine the criterion more precisely. Click the **[port]** and **[select IP Address]** successively to set their detail. See also: Select Ports and Select an IP address.
5. Back to the Rule Editor Wizard, click **Next** once conditions are set.

6. Enter a name and a description for the rule.



Rule Editor Wizard

Finish rule setup.

Step 1: Specify a name for this rule

Port Forwarding

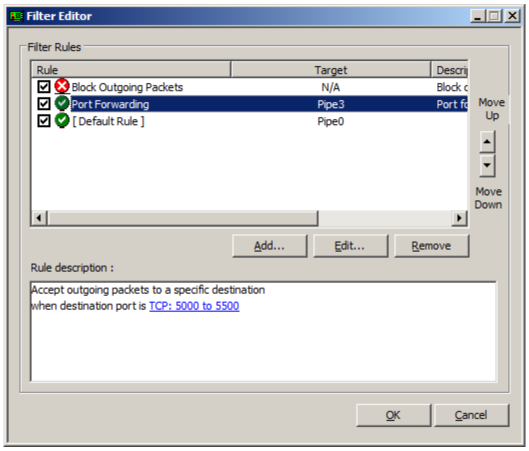
Step 2: Edit the rule description

Port forwarding to port range 5000-5500

Step 3: Select the targeted pipe for this rule

Pipe3

7. As shown, select a target from **Pipe1** to **Pipe7** where accepted packets are to be routed based on destination IP address and/or port setting(s). See note about Pipe0.
8. Click **Finish**. The new rule has now been added to the rule editor. As shown next, make sure the new rule is checked in order to make use of it.



Filter Editor

Filter Rules

Rule	Target	Descri
☑ Block Outgoing Packets	N/A	Block c
☑ Port Forwarding	Pipe3	Port fo
☑ [Default Rule]	Pipe0	

Rule description :

Accept outgoing packets to a specific destination
when destination port is TCP: 5000 to 5500

9. Select a rule and review settings in the lower pane. Click hyperlink(s) to last minute changes.
10. Select a rule, then use the up or down arrow to set rule prioritization.
11. Click **OK** to save the rules and close Filter Editor.
12. Right-click the functional group targeted by the newly defined accept-type rule and click **Publish Policies** to save in the system. The new rule will be applied to new mobile clients assigned to this group and to existing group clients as they reconnect to a Mult-IP Gateway.

Setting Rule Priority

Before applying a rule set, list each rule in priority sequence. For example, if you want to block packets from ports 1024 to 4026 but accept packets on port range 5000-5500 targeting Pipe3, while accepting packets from all other ports targeting Pipe0, you will need to add two rules to the default rule.

Note: Depending on how a rule is defined and prioritized, it may supersede and invalidate another without the user's knowledge. Users must exercise caution when handling rules to prevent rule scenarios that do not reflect expected packet behavior.

Rules created and sorted:

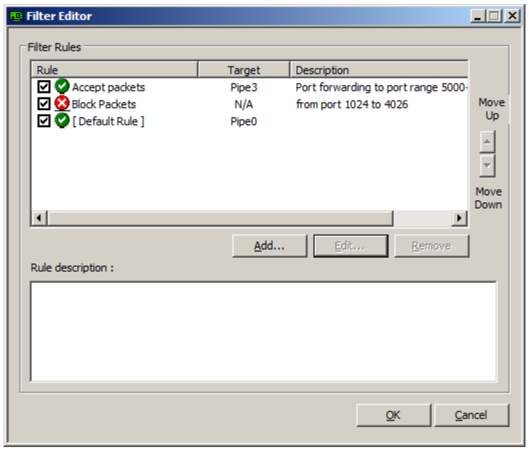
- Accept outgoing TCP packets pointing to IP 192.168.1.110 on port range 5000-5500 targeting **Pipe3**.
- Block outgoing packets from ports 1024 to 4026.
- Default rule (Accept all outgoing ports to **Pipe0**).

New rules apply to new mobile clients joining the functional group or to existing group clients as soon as their connection is reset.

Warning: The default rule is always active and cannot be removed.

To set rule priority,

1. To set rule priority, select a rule and click the **Move Up** or **Move Down** arrow.



Rule	Target	Description
☑ ✓ Accept packets	Pipe3	Port forwarding to port range 5000-
☑ ✗ Block Packets	N/A	from port 1024 to 4026
☑ ✓ [Default Rule]	Pipe0	

2. Double-check filter settings, then right-click the target functional group and select **Publish Policies**. New rules will be saved in system storage and pushed to clients the next time they reconnect.

Editing or Removing Rules

- To edit a rule, select it and click **Edit** (or double-click the rule) and make the necessary modifications. Back to the Filter Editor, click **OK**.
- To remove a rule, select the rule, click **Remove** and click **OK**.
- Right-click the functional group managed by the updated rule set and select **Publish Policies** to save to the system file. Clients will apply changes the next time they connect.

Deployment Scenario

This section is a practical guide to principles defined in Controlling Traffic. It is intended to help you better understand concurrent network management through a typical case scenario in which pipes are matched with filter rules to optimize the use of established private narrowband network(s) alongside broadband networks. This scenario will be kept simple, merging extreme usage situations in a single process. Doing so should clearly demonstrate how field practices affect the decision-making process involved at every step of the way.

Note: This scenario focuses on concurrent networking and filter management. All work leading to this point, which involves breaking down the fleet into functional groups as well as configuring all available communication drivers is assumed complete.

Step One: address agency needs

As a mandatory first step, let us consider the communication needs of a *First Responders* agency's client workstations. The following points highlight a typical decision-making process.

Let us pool the applications that fall within the mandate of first responders and paramedics:

- CAD (Computer Aided Dispatch)
- Vehicle Locator
- HTTP/internet browsing
- FTP
- Electronic Medical Record (EMR) transfers telepresence

Next, we must consider the data communication systems available to the *First Responders* agency that is best suited to meet those requirements:

- **Wi-Fi**: The most obvious network. Usually not available in a moving vehicle, it offers stationary vehicles inexpensive access to broadband internet for such purposes as downloading software and antivirus updates, telepresence (high-res photo and video) as well as EMRs (Electronic Medical Records) uploads.
- **Public Cellular HSPA**: For access to broadband on-the-go, client workstations are equipped with broadband cellular HSPA dongles suitable for HTTP, instant access to medical records, upload of diagnostic images, and so on. In addition, low latency cellular networks offer economies of scale by supporting VOIP software for calls to landlines of extended durations. Broadband cellular is subject to traffic caps imposed by network providers.
- **Motorola HPD™**: The *First Responders* agency leverages the city's investment in the Astro 25 standard primarily set up for P25 voice, making HPD an essential component of the fleet's mission-critical nature despite its relatively narrow bandwidth. After extensive deployment, the city is "blanketed" with a solid network of repeaters offering total coverage. While it is not suitable for broadband traffic, it remains immune to peak data usage and is a reliable outlet for such applications as CAD, text messaging, client identification and tracking as well as text-based database lookup and field reporting.

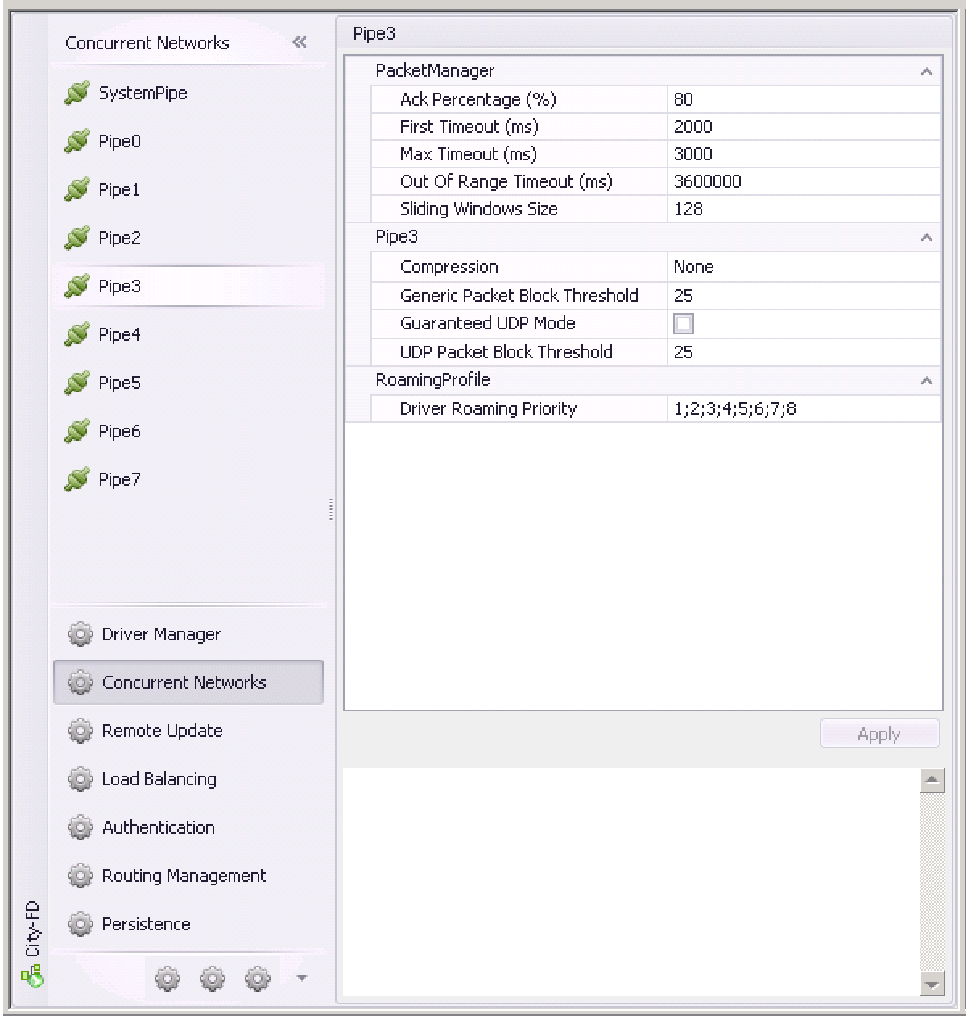
Step Two: configure concurrent networks

With agency requirements set, the system administrator logs on to the Mult-IP management console and decides which networks (or communication drivers) are best suited to work together over a given pipe on the basis of each pipe's data usage and each driver's known characteristics and service area.

To configure concurrent networks,

1. Log on to the management console with appropriate privileges and navigate to the *First Responders* functional group (presumably created earlier).
2. With the **DriverManager** tab highlighted, acknowledge communication driver entries for **001-Generic IP**, **002-Celllular HSPA, 003-Wi-Fi** and **004-Motorola HPD** drivers as per requirements expressed in Step One. Take note of the **Driver index** value for each communication driver, you will refer to it later.
3. Click **Concurrent Networks** and select **Pipe3**. In keeping with our scenario, we will assign **Pipe3** to high bandwidth multimedia (streaming video, high-resolution image download and miscellaneous electronic medical record transactions).

Note: Keep in mind that remote updates are also transferred on **Pipe3**, so take in account the communication driver performance.



Pipe3

PacketManager	
Ack Percentage (%)	80
First Timeout (ms)	2000
Max Timeout (ms)	3000
Out Of Range Timeout (ms)	3600000
Sliding Windows Size	128
Pipe3	
Compression	None
Generic Packet Block Threshold	25
Guaranteed UDP Mode	☐
UDP Packet Block Threshold	25
RoamingProfile	
Driver Roaming Priority	1;2;3;4;5;6;7;8

4. Click **Driver Roaming Priority** and replace the default roaming parameter sequence (1;2;3;….8) with the preferred communication driver polling sequence. This will later result in a policy update that will inform mobile clients of the preferred order in which communication drivers are used in this pipe. In our typical case scenario, type 2;3 to involve Cellular HSPA and Wi-FI drivers for broadband use in our roaming scenario.
5. Move to the **PacketManager** section in Concurrent Network tab and apply settings that will accommodate the communication driver used more often in your roaming scenario, which in our example would be the Cellular HSPA. Here are a few numbers to consider based on in-house tests:
   a) **Ack Percentage (%):** 40
   b) **First Timeout (ms)**: 200
   c) **Max Timeout (ms)**: 500
   d) **Sliding Windows Size**: 64
6. Click **Apply** to save pipe settings.
7. Click **Pipe2**, This pipe will be dedicated to web traffic. Repeat steps 3 to 6 to configure pipe attributes, paying attention to the following practical considerations:
   a) Have Driver index values at hand and set **Driver Roaming Priority** to 3;2, putting the Wi-Fi driver ahead of Public Cellular HSPA. The reasoning being that frequent roaming will not significantly affect web browsing.
   b) Move to the **Pipe2** portlet and enable **Compression**. This may contribute to speed improvements in some instances.
   c) Set **Ack Percentage (%)** to 60.
   d) Set **First Timeout (ms)** to 500
   e) Set **Max Timeout (ms)** to 1500
8. Click **Apply** to save pipe settings.
9. Click **Pipe1** and configure attributes to meet the narrowband requirements of sensitive applications such as CAD.
   a) Set **Driver Roaming Priority to** 3;2;4 to allow narrowband traffic (set later in filter rules) on all communication drivers. Motorola HPD is used when all other networks are unusable.
   b) Move to **PacketManager** and set **Sliding Windows Size** to **32**. Set all values to the specifications of the narrowband driver's modem supplier despite the fact that all communication drivers are employed. In our current scenario, merging broad and narrowband networks on one pipe requires that we enforce performance characteristics of the more resilient narrowband Motorola HPD driver.
   c) Move to the **Pipe1** portlet and enable **Compression**. Compressing text-type traffic will greatly improve performance on the narrowband network.
10. Click **Apply** to save pipe settings. By now, pipes 1, 2 and 3 are fully configured and ready to handle incoming traffic routed by way of the filter rules defined next.

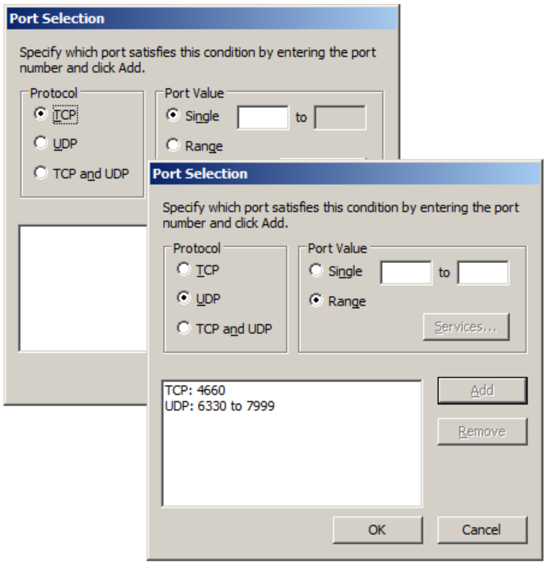
Step Three: define filter rules

Rules are designed to *accept*, *reject* or *drop* incoming client packets, then to route accepted packets to a destination IP address and port via a specific pipe. In keeping with corporate requirements set earlier in Step One, define the following rules.

- Accept narrowband packets and send to a destination IP address through **Pipe1**;
- Accept packets destined to port 80 (HTTP) and route through **Pipe2**;
- Accept high traffic (streaming video, EMR, FTP) to specific IP/port destinations through **Pipe3**;
- Block all other packets.

Rule 1: Allow narrowband traffic through Pipe 1

1. Select the **First Responders** functional group and click **Launch Filter Editor** in the Actions pane.
2. Click **Add** in the main window, and then select the **Accept outgoing packets to a specific destination** template followed by **Next** to launch the rule definition wizard.
3. Check the **On Destination port match** condition, and then click the **Port** hyperlink in the lower pane to display the next port selection screen.



Port Selection

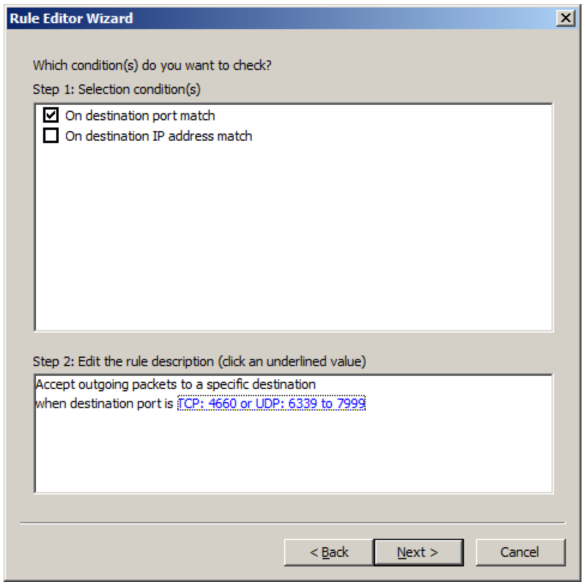
Specify which port satisfies this condition by entering the port number and click Add.

Protocol: ○ TCP ● UDP ○ TCP and UDP

Port Value: ○ Single ● Range

TCP: 4660
UDP: 6330 to 7999

4. As shown above, add TCP and/or UDP ports used by CAD software. Click **Add** once individual modes are set, then click **OK** to close window.



Rule Editor Wizard

Which condition(s) do you want to check?

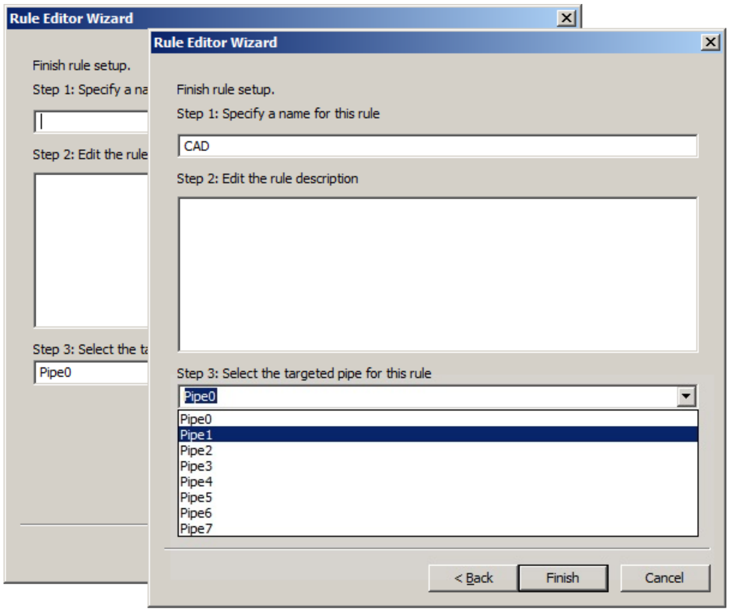
Step 1: Selection condition(s)

☑ On destination port match
☐ On destination IP address match

Step 2: Edit the rule description (click an underlined value)

Accept outgoing packets to a specific destination
when destination port is TCP: 4660 or UDP: 6339 to 7999

5. Back to the condition selection screen, review port selection (blue text), then click **Next**.



Rule Editor Wizard

Finish rule setup.

Step 1: Specify a name for this rule

CAD

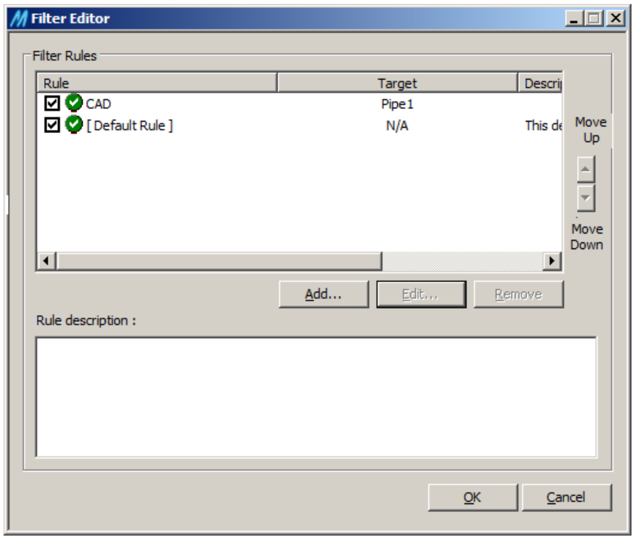
Step 2: Edit the rule description

Step 3: Select the targeted pipe for this rule

Pipe0

6. Type a name for the new rule, such as **CAD**. You may also append a brief description.
7. Select **Pipe1** from the drop-down list, and then click **Finish** to register the rule.

8. Back to the main GUI, click the checkbox next to the new **CAD** rule to enable. Your display should now look like this.

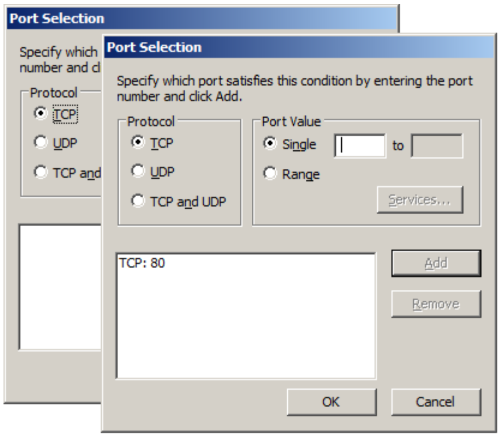


Rule	Target	Descri
☑ CAD	Pipe1	
☑ [Default Rule]	N/A	This de

9. At this point, click **Add** to create an additional rule.

Rule 2: Allow HTTP packets on port 80 through pipe 2

1. In the main Filter Editor window, click **Add**, then select the **Accept outgoing packets to a specific destination** template followed by **Next** to launch the rule definition wizard.
2. Click the **On Destination port match** checkbox, then click the **Port** hyperlink.



Port Selection

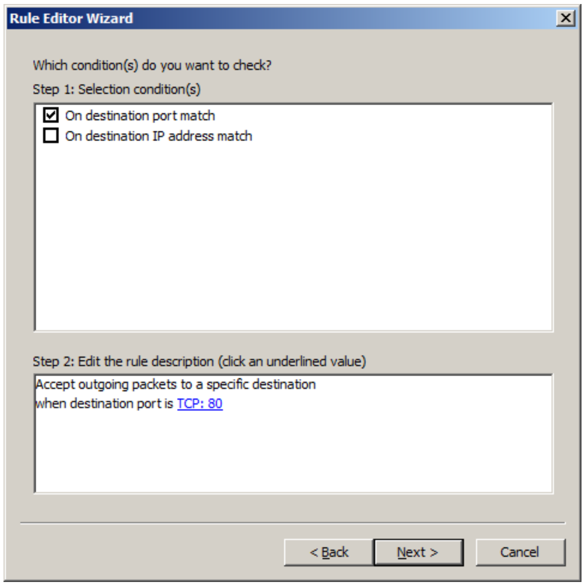
Specify which port satisfies this condition by entering the port number and click Add.

Protocol: ● TCP ○ UDP ○ TCP and UDP

Port Value: ● Single [ ] to [ ] ○ Range

TCP: 80

3. As shown, select both **TCP** and **Single** radio buttons then type **80** as the port value.
4. Click **Add** followed by **OK** to close window.



Rule Editor Wizard

Which condition(s) do you want to check?

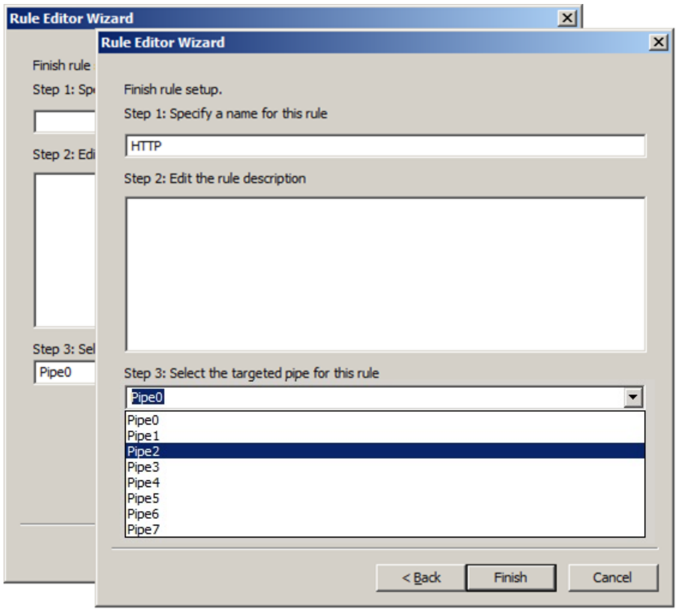
Step 1: Selection condition(s)

☑ On destination port match
□ On destination IP address match

Step 2: Edit the rule description (click an underlined value)

Accept outgoing packets to a specific destination
when destination port is TCP: 80

5. Back to the condition selection screen, review port selection(s) (blue text), then click **Next**.



Rule Editor Wizard

Finish rule setup.

Step 1: Specify a name for this rule

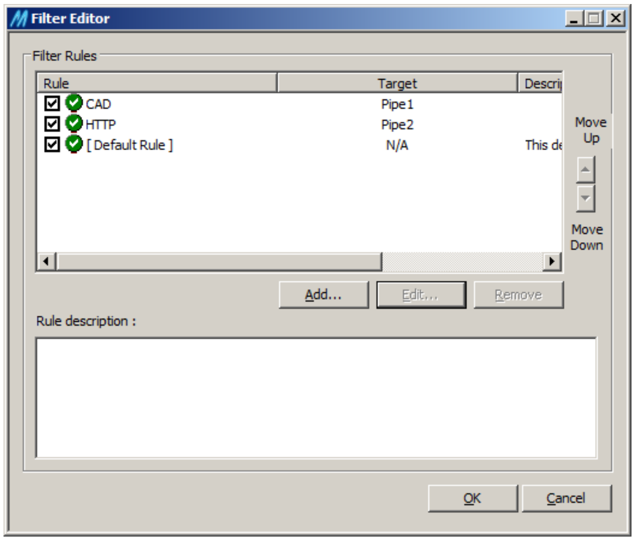
HTTP

Step 2: Edit the rule description

Step 3: Select the targeted pipe for this rule

Pipe0

6. As shown, type a rule name, such as **HTTP**, and provide an optional description.
7. Select **Pipe2** from the drop-down list, and then click **Finish** to register the rule.
8. Back to the main GUI, click the checkbox next to **HTTP** to enable the new rule resulting in the following display.



Filter Rules

Rule	Target	Descri
☑ CAD	Pipe1	
☑ HTTP	Pipe2	
☑ [Default Rule]	N/A	This de

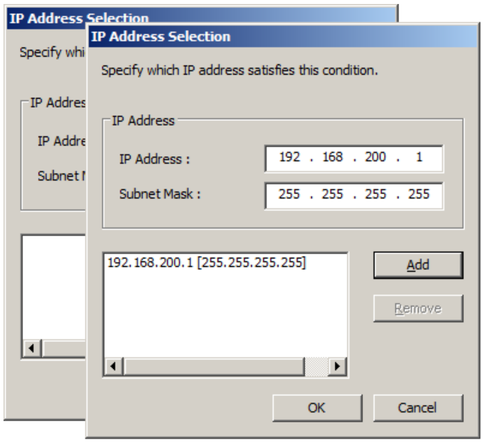
Rule description :

Rule 3: Allow broadband traffic through pipe 3

This elaborate rule specifies both destination IP and port to filter incoming packets.

Note: Remote updates sent over **Pipe3** are not affected by filter rules designed using this pipe.

1. Back to the main Filter Editor window, click **Add**, then select the **Accept outgoing packets to a specific destination** template followed by **Next** to launch the rule definition wizard.
2. Click both **On Destination port match** and **On destination IP address match** checkboxes. Doing so will require that both conditions are met for broadband traffic to be accepted.
3. Click the **select IP Address** hyperlink



IP Address Selection

Specify which IP address satisfies this condition.

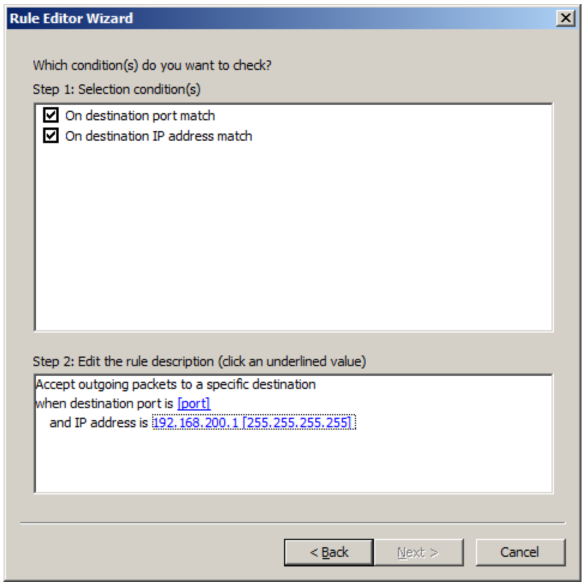
IP Address

IP Address : 192 . 168 . 200 . 1

Subnet Mask : 255 . 255 . 255 . 255

192.168.200.1 [255.255.255.255]

4. As shown, set the destination IP and subnet mask of a destination FTP/File server field workers will be downloading from or uploading to.
5. Click **Add** followed by **OK** to register destination and exit this screen. Your display should look like this.



Rule Editor Wizard

Which condition(s) do you want to check?

Step 1: Selection condition(s)

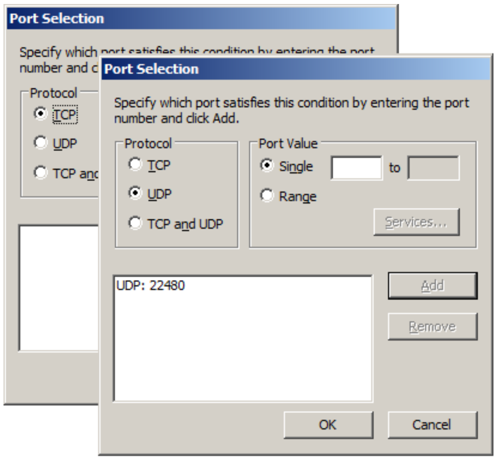
☑ On destination port match

☑ On destination IP address match

Step 2: Edit the rule description (click an underlined value)

Accept outgoing packets to a specific destination
when destination port is [port]
and IP address is 192.168.200.1 [255.255.255.255]

6. Repeat the previous two steps for all servers you wish to make available, then click **OK**.
7. Back to the condition selection screen, click the port hyperlink.



Port Selection

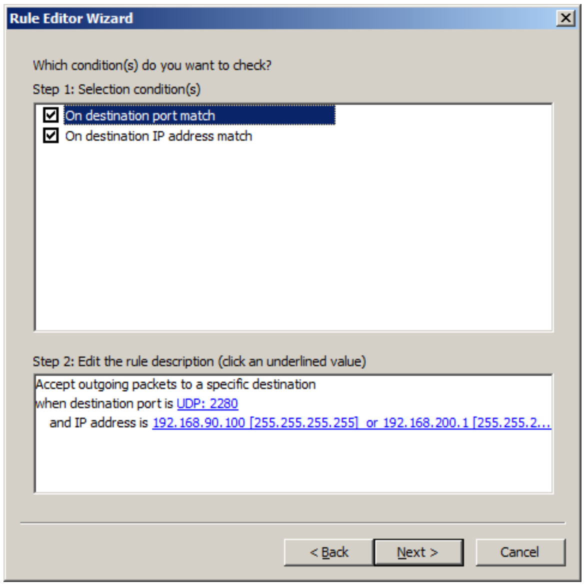
Specify which port satisfies this condition by entering the port number and click Add.

Protocol: ○ TCP ● UDP ○ TCP and UDP

Port Value: ● Single [ ] to [ ] ○ Range

UDP: 22480

8. As shown, click **UDP** and type the port (or port range) you wish to keep open to file transfer traffic through your corporate firewall, then click **Add.** Again, you may add all individual ports (or port ranges) needed for foreseeable applications, then click **OK** to close window.



Rule Editor Wizard

Which condition(s) do you want to check?

Step 1: Selection condition(s)

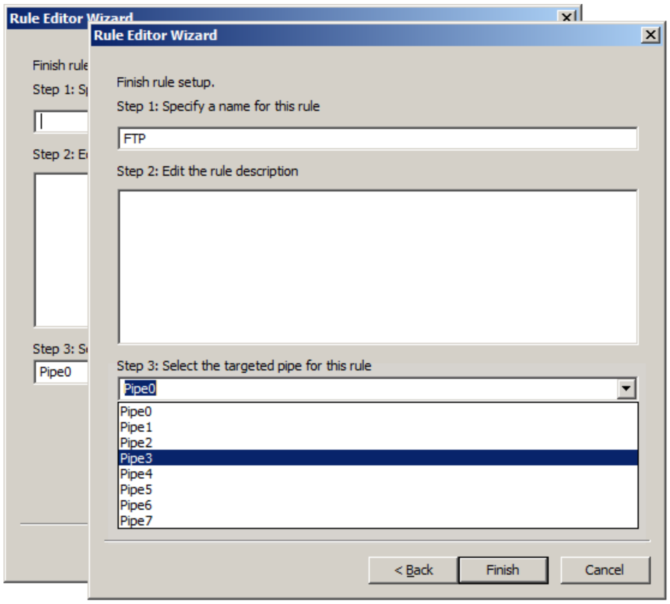
☑ On destination port match

☑ On destination IP address match

Step 2: Edit the rule description (click an underlined value)

Accept outgoing packets to a specific destination
when destination port is UDP: 2280
and IP address is 192.168.90.100 [255.255.255.255] or 192.168.200.1 [255.255.2...

9. Back to the condition selection screen, review rule description (blue text), then click **Next**.



Rule Editor Wizard

Finish rule setup.

Step 1: Specify a name for this rule

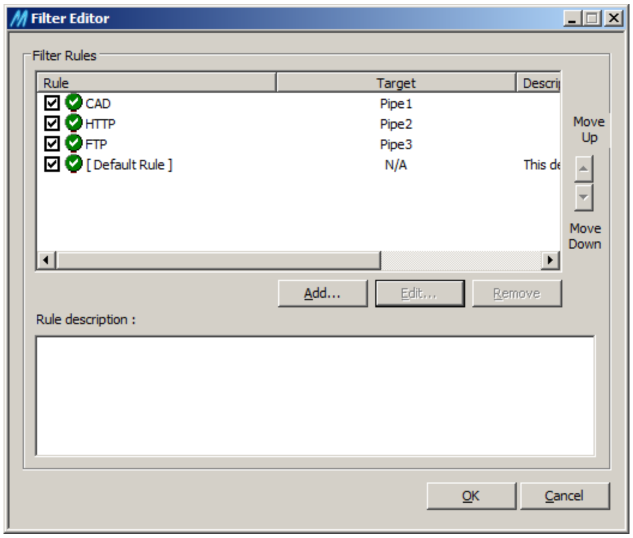
FTP

Step 2: Edit the rule description

Step 3: Select the targeted pipe for this rule

Pipe0

10. Type a name for the new rule, such as **FTP**, and supply an optional description.
11. Select **Pipe3** from the drop-down list, and then click **Finish** to register the rule.
12. Back to the main GUI, click the **FTP** checkbox to enable the new rule. The rule set defined so far should appear as shown on the next screen sample:



Filter Editor

Filter Rules

Rule	Target	Descri
☑ ✓ CAD	Pipe1	
☑ ✓ HTTP	Pipe2	
☑ ✓ FTP	Pipe3	
☑ ✓ [Default Rule]	N/A	This de

Rule description :

Rule 4: Block unwanted traffic

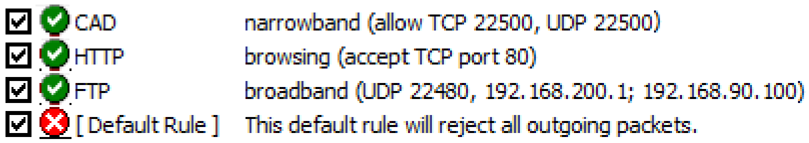
Note: This last procedure applies to the built-in default rule. Contrary to rules created from scratch, the default rule accepts all incoming packets, or else, rejects or drops all packets whose destination was not set as part of custom accept-type rule definition.

1. In the main Filter Editor window, select **Default Rule** then click **Edit**.
2. Choose from one of the available options:
   a) Click **Accept all packets** to allow packets whose destination is not accounted for in any set rule to be allowed over the default pipe. This option is not recommended.
   a) Click **Reject all packets** (or **Drop all packets**) to block packets. Jump to page 71 to learn how the two selections differ.
3. Click **OK** to update default rule behavior.

Step Four: enable filter rules

At this stage, we can assume that pipes and filters are fully configured. However before deploying those related settings to clients, review how rules break down from top to bottom and make sure there is no overlapping to avoid conflicts.

Consider the list of rules defined as part of this exercise:



☑ ✓ CAD	narrowband (allow TCP 22500, UDP 22500)
☑ ✓ HTTP	browsing (accept TCP port 80)
☑ ✓ FTP	broadband (UDP 22480, 192.168.200.1; 192.168.90.100)
☑ ✗ [Default Rule]	This default rule will reject all outgoing packets.

As stated earlier in Controlling Traffic, rule evaluation is performed with the first rule checked for relevancy to incoming packets. Packet evaluation then moves to the second and third rule until it is blocked by the last rule simply because no match was found.

Looking at the above rule set reveals no conflicts. In other words, each rule covers an exclusive IP or port value (or range) and can be applied as is. Furthermore, as described in the default rule, any packet not matching previously expressed condition will be rejected.

Step Five: push new policies to clients

To apply all the configurations described in this sample scenario,

1. Right-click the **First Responders** functional group and click **Publish Policies** to save the latest filter rule definitions into system storage.
2. To deploy filter rules to group clients, you may select the **Clients** node and, from the client list workspace, force a Reset connection on selected clients. You may also ask users to perform a **Reset Connection** at a suitable time.

Managing Mobile Devices

This section focuses on operational tasks related to fleet management. While most features apply equally to single-gateway or load-balancing topologies, some are exclusive to a load-balancing environment and will be clearly indicated.

Processing New Client Connections

Allowing clients into your VPN environment is not something that should be treated lightly. That is why Mult-IP is designed to process incoming client connections in one of two ways:

- **By default, the system is set to quarantine unknown mobile devices.** To accomplish this, a *Quarantine* group is created during installation of the Mult-IP software (see below). Its purpose is to provide a holding area for all clients on their first connection, preventing them from accessing system resources until they have been manually acknowledged and moved to a functional group by a console operator.
- **Clients can be automatically allowed into the system.** When conditions warrant, such as when performing bulk fleet deployment, use the Set as default group feature to specify a destination group that will automatically accept all incoming new connections. This process bypasses quarantine mode and allows clients to download policies configured and published for the destination group.

Regardless of your preference for one of the above-connection targets, keep in mind that clients must reach a specified destination upon initial registration. Review the following table which identifies group graphical representations in order to help quickly track what group is set as a default target:

✓🟥	**Quarantine group set as default**. All clients join this group upon initial registration pending operator acknowledgement. This is the default behavior.
🟥	**Quarantine group suspended**. While not-yet-acknowledged clients may still be held in this group (not yet acknowledged by operator), Mult-IP no longer allows clients due to a group assignment change.
✓🟩	**Functional group set as default**. Incoming clients are automatically assigned to this group and inherit group policies.
🟩	**Functional group secure**. Clients are assigned to this group and inherit its policies only once they have been acknowledged by operator.

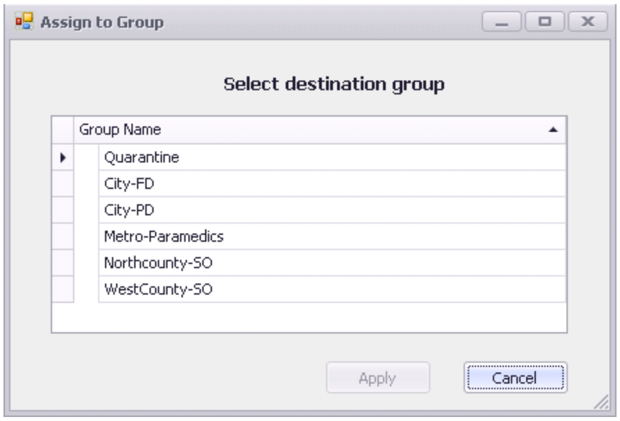
Note: Unlike functional groups that can be added and deleted at will, the *Quarantine* group is built-in. As such, it can be used as the default group or not, however it cannot be deleted.

Assigning Clients to Functional Groups

This section will show you how to browse the Client list and assign new mobile client connections to functional groups. To this end, it is assumed that Mult-IP is set to the default behavior of assigning all new connections to a Quarantined group pending operator acknowledgement.

To assign a client to its functional group,

1. Log on to the management console with group administration privileges and click the **Clients** node. Look for clients marked as **Quarantine** in the **Group** column or to clients you wish to reassign to a new group.
2. Highlight a single or a group of clients, and then select **Assign to Group** from the Actions pane to display the following selection screen.



Group Name
Quarantine
City-FD
City-PD
Metro-Paramedics
Northcounty-SO
WestCounty-SO

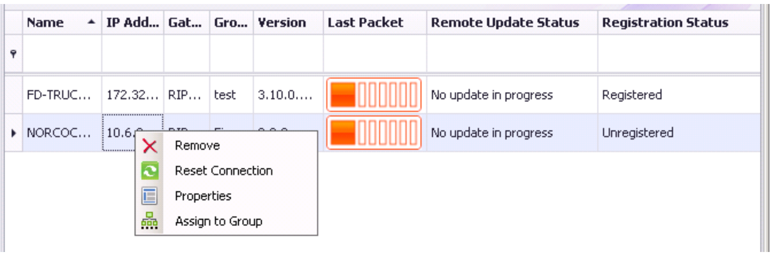
3. Select the group to which the client(s) will be assigned.
4. Click **Apply**. A command will immediately be issued to the selected client(s), prompting a move from *Quarantine* to the new group. Depending on the wireless network used, you may need to allow some time for this process to complete and for client to apply policies defined for the target functional group.

Viewing Client Properties

The Properties viewer is intended to focus your attention on a specific client by displaying a wide range of real-time updated information for monitoring or troubleshooting purposes. While most entries are read-only, this view supports such tasks as [assigning client to group]() or [enforcing IP address reservation]().

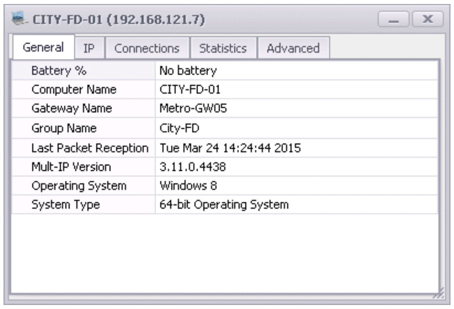
To display client properties,

1. As shown next, click the **Clients** node, then right-click any active client.



Name	IP Add...	Gat...	Gro...	Version	Last Packet	Remote Update Status	Registration Status
FD-TRUC...	172.32...	RIP...	test	3.10.0....	▮▯▯▯▯▯▯▯	No update in progress	Registered
NORCOC...	10.6.				▮▯▯▯▯▯▯▯	No update in progress	Unregistered

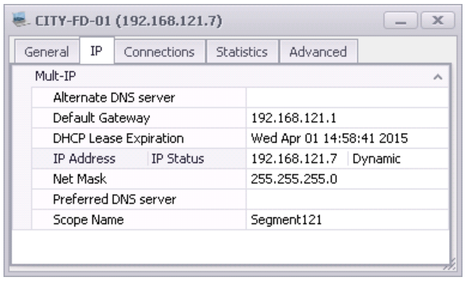
2. Select **Properties** from the context menu to display contents.
3. Click on any tab to view (or sometimes edit) sorted parameters.



Battery %	No battery
Computer Name	CITY-FD-01
Gateway Name	Metro-GW05
Group Name	City-FD
Last Packet Reception	Tue Mar 24 14:24:44 2015
Mult-IP Version	3.11.0.4438
Operating System	Windows 8
System Type	64-bit Operating System

Click the **General** tab to:

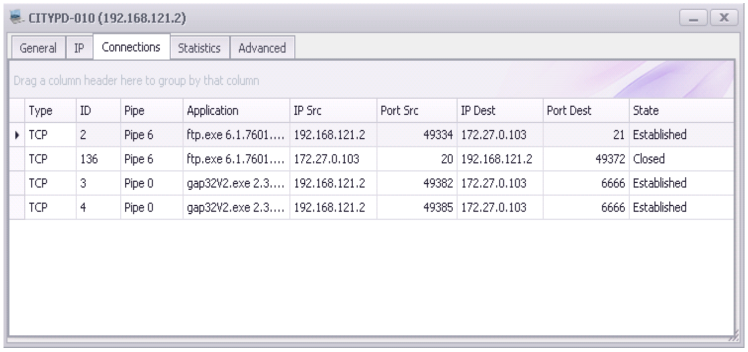
- View client and OS version info;
- View date and time of last received packet. (**Note**: this information is unique to this view.);
- Assign to a new functional group.



Mult-IP		
Alternate DNS server		
Default Gateway	192.168.121.1	
DHCP Lease Expiration	Wed Apr 01 14:58:41 2015	
IP Address / IP Status	192.168.121.7	Dynamic
Net Mask	255.255.255.0	
Preferred DNS server		
Scope Name	Segment121	

Click the **IP** tab to:

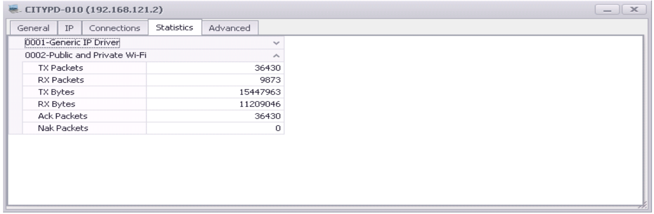
- View current IP and DNS info applied to the client's Virtual Network Interface Card (VNIC).
- Find the information about the DHCP lease expiration


CITYPD-010 (192.168.121.2)
General
IP
Connections
Statistics
Advanced
Drag a column header here to group by that column

Type	ID	Pipe	Application	IP Src	Port Src	IP Dest	Port Dest	State
TCP	2	Pipe 6	ftp.exe 6.1.7601....	192.168.121.2	49334	172.27.0.103	21	Established
TCP	136	Pipe 6	ftp.exe 6.1.7601....	172.27.0.103	20	192.168.121.2	49372	Closed
TCP	3	Pipe 0	gap32V2.exe 2.3....	192.168.121.2	49382	172.27.0.103	6666	Established
TCP	4	Pipe 0	gap32V2.exe 2.3....	192.168.121.2	49385	172.27.0.103	6666	Established

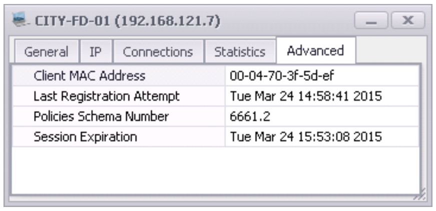
Click the **Connection** tab to:

- Break down TCP and UDP data flows;
- Monitor port assignments;
- Monitor pipe transfers and ultimately determine if filter rules properly apply (if applicable).



0001-Generic IP Driver	
0002-Public and Private Wi-Fi	
TX Packets	36430
RX Packets	9873
TX Bytes	15447963
RX Bytes	11209046
Ack Packets	36430
Nak Packets	0

Click the **Statistics** tab to view the total amount of packets transferred and received (from the client end) cumulated during the course of the current session.



Client MAC Address	00-04-70-3f-5d-ef
Last Registration Attempt	Tue Mar 24 14:58:41 2015
Policies Schema Number	6661.2
Session Expiration	Tue Mar 24 15:53:08 2015

Click the **Advanced** tab to view the virtual MAC address assigned to each client and its connected gateway through the Virtual Network Interface card.

The field Policies Schema Number shows the current version of the group policies in use by a particular client. If it doesn't match the one in the group, a reset connection could be forced to bring the client up to date.

Encryption

Information transiting through Mult-IP is encrypted end-to-end using cryptographic algorithms. In addition, Mult-IP supports secure connection from the start by applying a handshake protocol between gateway and client that requires that both parties agree on the rules of further transmission.

The type of encryption applies system-wide; it is determined as part of your product license and cannot be segregated among functional groups. The choice of which encryption method (or cypher) best applies to your environment depends on application robustness and availability may be subject to export rights outside the US and Canada. The System Info tab of the Mult-IP Dashboard indicates the active encryption algorithm.

Supported encryption algorithms include :

- No encryption
- Triple DES
- Single DES
- AES 128 bits
- AES 192 bits
- AES 256

Note: Your Mult-IP system comes preconfigured to DES_MS encryption.

Authentication

Authentication is the process of validating user identity before granting access to corporate resources. While most computer systems actively enforce authentication by requesting a user name and password combination, Mult-IP defers the authentication process to an external security authority. In this manner, organizations are dispensed from having to rethink their authentication policies by simply integrating the new Mult-IP Mobile VPN to existing Windows-based or RADIUS methods.

Authentication is performed during mobile client registration. Once connected and registered to a gateway, users are considered logged on and authenticated, even if the authentication settings change in the course of an active work session, for example, when the Mult-IP system administrator decides to change an existing group policy from a Radius type policy to a 802.1X one. Furthermore, if the mobile client goes out of range of any radio network, the user will remain authenticated over a configurable amount of time allowed for machine session persistence. However, initiating a **Reset Connection** will force authentication renewal by allowing new authentication policies to take effect upon workstation registration.

When user authentication must be performed (for example against LDAP) before the Mult-IP MVPN is fully established, then Pre-Authentication filters must be defined. Refer to the Pre-Authentication filters section.

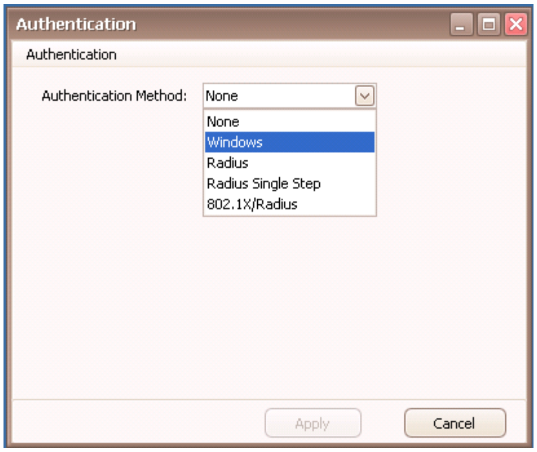
Notice about field validation: as you browse through the following subsections, keep in mind that authentication field entries are validated as you type. From the moment an authentication window is open, you may only click **Cancel** if all fields are empty or some of them contain admissible values. You may only click **Apply** once all fields contain admissible values.

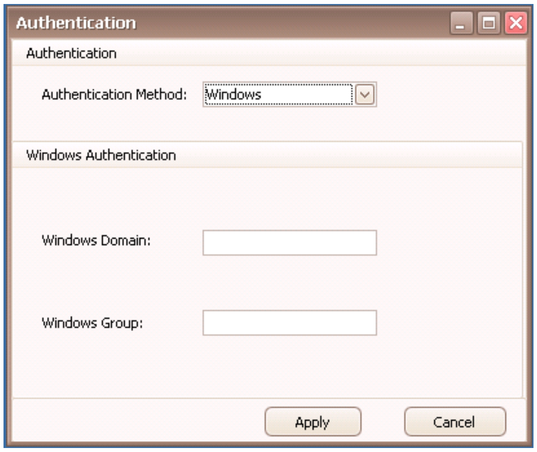
Windows Authentication

Windows authentication leverages client/server security features built in the Windows OS. Once published to mobile clients, the local Windows OS prompts users to enter their username/password upon connection to a Mult-IP Gateway. Credentials are sent over the air to be validated against those contained in the corporate Active Directory accessible to the Mult-IP Gateway via the corporate LAN.

To enable Windows-based Authentication,

1. Log on to the management console with sufficient privileges and expand the **Policies** >**Client Policies** nodes.
2. Right-click the target functional group and select **Authentication** from the context menu to display the main Authentication selection window.

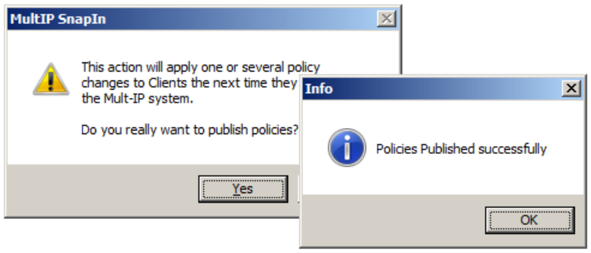

Authentication
Authentication
Authentication Method: None


Authentication
Authentication
Authentication Method: Windows
Windows Authentication
Windows Domain:
Windows Group:

3. As shown, select **Windows** from the **Authentication Method** drop-down list.
4. Type the **Windows Domain** that uses a domain server to manages users. This field identifies where the authentication request will be forwarded. Leaving blank, or entering the machine name of any Mult-IP Gateway would require this computer to authenticate users locally.

Note: Domain authentication requires that all Mult-IP Gateways be located within the domain itself.

5. Type the Windows organizational unit (group) to identify a subset of users. When specifying a group, the authentication process only accepts users that are members of this group. If a user is member of the specified group, then authentication will be processed.
6. Once you are satisfied with your authentication settings, click **Apply** to save changes.
7. Again, right-click the target functional group and select **Publish Policies.** Wait for the next confirmation message.


MultIP SnapIn
This action will apply one or several policy changes to Clients the next time they the Mult-IP system.

Do you really want to publish policies?

Info
Policies Published successfully

8. Click **Yes** followed by **OK**. The new Windows authentication method will be saved as new policies that will be applied to new mobile clients assigned to this functional group or to existing group clients reconnecting to a Mult-IP Gateway using Reset Connection.

Radius Authentication

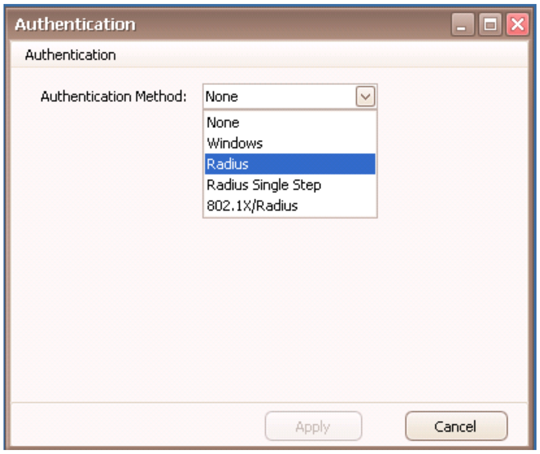
The Radius protocol is designed to allow NAS (Network Access Service) to validate user credentials against a centralized database. The flexibility and scalability of Radius supports various authentication protocols (like EAP, PEAP, CHAP, PAP, and so on) and contributes to make it an industry standard. Radius servers, also referred to as AAA servers, provide Authentication, Authorization and Accounting.

Note: Make sure that your Radius server can handle PAP. Also make sure Radius server and Mult-IP Gateways are on the same IP segment and that Radius recognizes all Mult-IP Gateway host IPs as valid Radius clients.

Note: To provide enhanced fault tolerance, it is possible to install a local Radius server acting as a proxy-forwarding request to a Radius server group.

To activate Radius authentication,

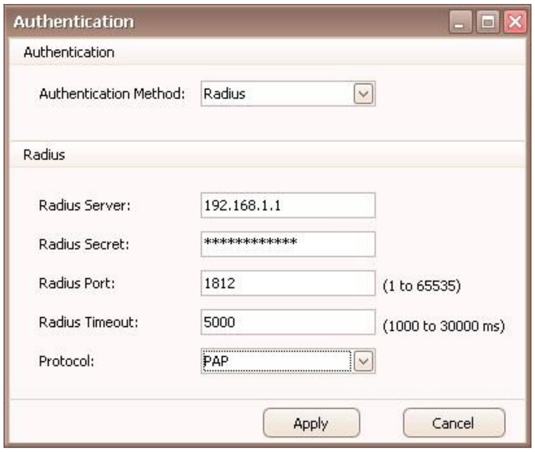
1. Log on to the management console with sufficient privileges and expand the **Policies** and **Client Policies** nodes.
2. Right-click a target functional group and select **Authentication** from the context menu to display the main Authentication selection window.



Authentication

Authentication

Authentication Method: None



Authentication

Authentication

Authentication Method: Radius

Radius

Radius Server: 192.168.1.1

Radius Secret: ************

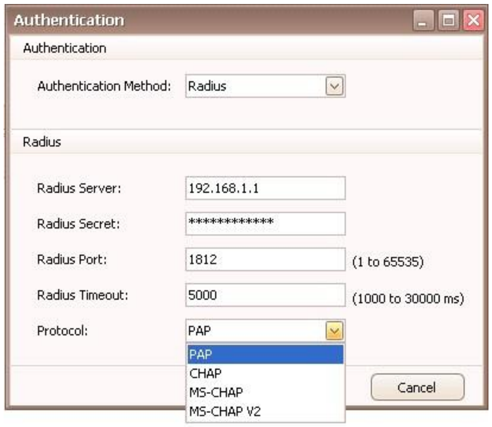
Radius Port: 1812 (1 to 65535)

Radius Timeout: 5000 (1000 to 30000 ms)

Protocol: PAP

3. Select **Radius** from the **Authentication Method** drop-down list and set fields as described next:
   a) Type the static IP address of the Radius server machine in the **Radius Server** field.
   b) Click the **Radius Secret** field and type the text string used as a password between the Mult-IP Gateways and the Radius server.
   c) Type the port number reserved for communication with Radius server software.
   d) Click the **Radius Timeout** field and type the amount of time (ranging from 1000 to 30000 milliseconds) allowed for response from the Radius server to an authentication request. Failure to respond within the set timeframe will result in an authentication error message returned to the mobile client.

e) Select the **Protocol** you want to use with you Radius server in the following drop-down list:



Authentication

Authentication Method: Radius

Radius

Radius Server: 192.168.1.1

Radius Secret: ************

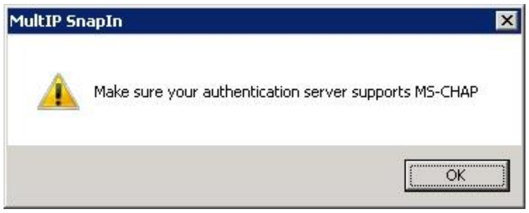
Radius Port: 1812 (1 to 65535)

Radius Timeout: 5000 (1000 to 30000 ms)

Protocol: PAP

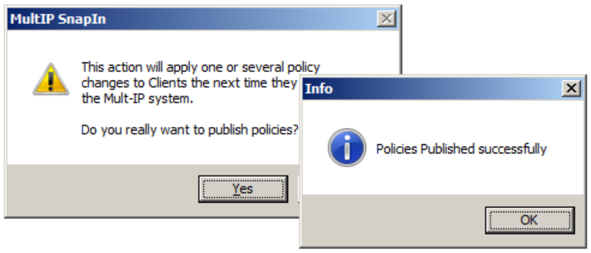
PAP
CHAP
MS-CHAP
MS-CHAP V2

4. Make sure your authentication server supports the protocol you have selected, as reminds you the following pop-up window:



Make sure your authentication server supports MS-CHAP

5. Once you are satisfied with your authentication settings, click **Apply** to save changes and close the window.
6. Again, right-click the target functional group and select **Publish Policies.** Wait for the next confirmation message.



This action will apply one or several policy changes to Clients the next time they the Mult-IP system.

Do you really want to publish policies?

Policies Published successfully

7. Click **Yes** followed by **OK.** The new Radius authentication method will be saved as new policies that will be applied to new mobile clients assigned to this functional group or to existing group clients reconnecting to a Mult-IP Gateway using Reset Connection.

Radius Single Step Authentication

This method should be selected if you wish to authenticate clients with two factors in a single step.

Support for two-factor hardware or software token authentication involves an extended authenticator with embedded Radius server for interfacing with the gateways acting as Radius clients. Keep in mind that from a security standpoint, once registered as a Radius client (or multiple Radius clients in case multiple gateways are used), the Mult-IP Gateways are transparent to the authentication process. You should therefore refer to your extended authenticator documentation for the practical aspects administration.

Interfacing extended authenticator with Mult-IP involves these three basic steps:

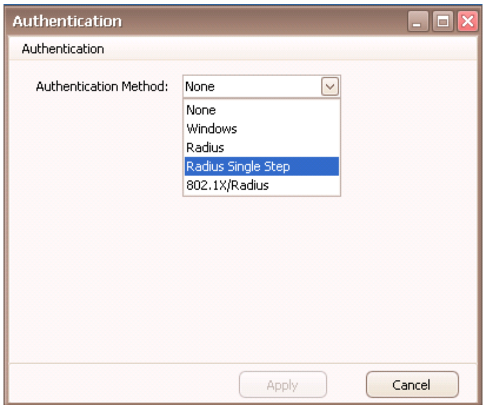
- Adding all Mult-IP Gateways as Radius clients to the extended authenticator.
- Setting up extended authentication for each target functional group.
- Publishing new authentication policies to target functional groups and performing a Reset Connection on mobile clients to force policies to apply, forcing authentication to take effect.

To add Mult-IP Gateways as Radius Clients,

1. Log on to your Extended authentication managing console and register all Mult-IP Gateway host IPs on the same IP segment as Radius clients.
2. Type the shared Radius secret to be shared with Mult-IP. Leave all other settings to default.
3. Save your changes and repeat this process for all IP addresses you wish to add as Radius clients.

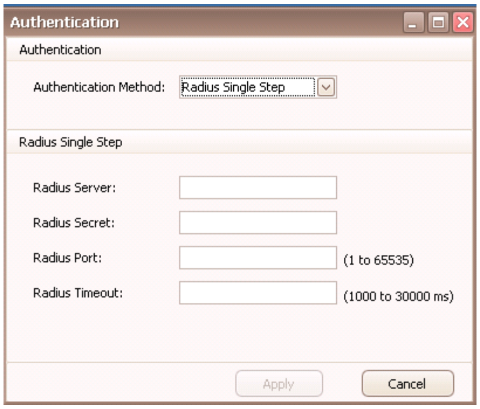
To set up Radius Single Step authentication for individual functional groups,

1. Log on to the management console with sufficient privileges and expand the **Policies** and **Client Policies** nodes.
2. Right-click a target functional group and select **Authentication** from the context menu to display the main Authentication selection window.


Authentication

Authentication

Authentication Method: None


Authentication

Authentication

Authentication Method: Radius Single Step

Radius Single Step

Radius Server:

Radius Secret:

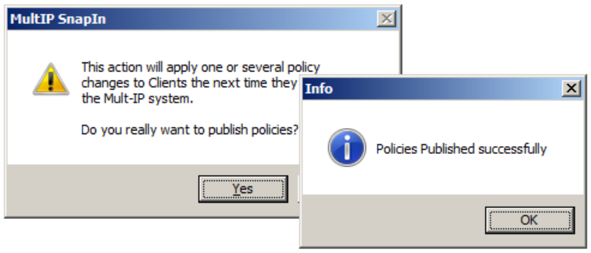
Radius Port: (1 to 65535)

Radius Timeout: (1000 to 30000 ms)

3. As shown, select **Radius Single Step** from the drop-down list and supply Radius Single Step information as described next.
   a) Type the static IP address of the physical machine running the extended authentication with embedded Radius Server in the **Radius Server** field.
   b) Click the **Radius Secret** field and type the text string used as a password shared between the Mult-IP Gateways and the Radius server.
   c) Type the port number reserved for communication with the Radius server software.

d) Click the **Radius Timeout** field and type the amount of time (ranging from 1000 to 30000 milliseconds) allowed for response from the Radius server to an authentication request. Failure to respond within the set timeframe will result in an authentication error message returned to the mobile client.

4. Once you are satisfied with your settings, click **Apply** to save changes and close the window.
5. Again, right-click the target functional group and select **Publish Policies.** Wait for the next confirmation message.



This action will apply one or several policy changes to Clients the next time they the Mult-IP system.

Do you really want to publish policies?

Policies Published successfully

6. Click **Yes** followed by **OK**. The new extended authentication method will be saved as new policies that will be applied to new mobile clients assigned to this functional group or to existing group clients reconnecting to a Mult-IP Gateway using Reset Connection.

802.1x Authentication

The 802.1x protocol is an advanced method that specifies a three-tier authentication mechanism composed of the client (supplicant), access controller (authenticator), and an authentication server. 802.1x specifies the use of EAP (Extensible Authentication Protocol) to validate the client's credentials against a Radius server.

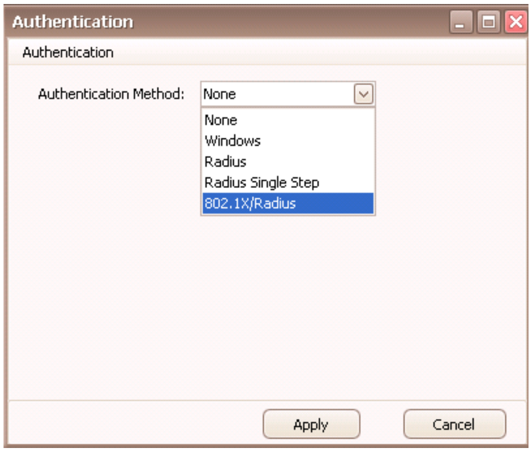
Mult-IP implements 802.1x by behaving as an access point that opens and closes the communication channels independently for each virtual port (client connection). Through 802.1x / EAP, Mult-IP can provide advanced authentication and perform mutual authentication of both authentication peers.

Notes:

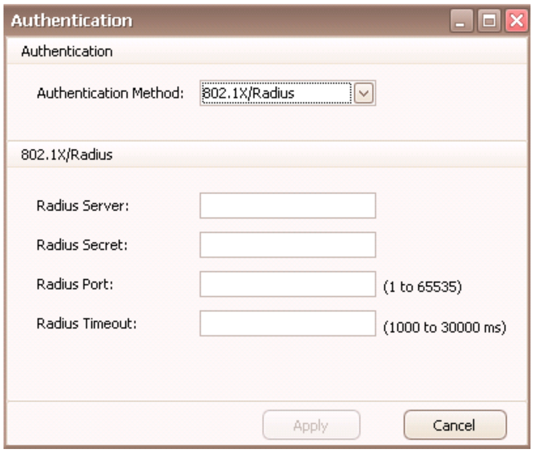
- 802.1x / EAP adds payload since it requires multiple exchanges to fully perform the authentication process. This authentication method may not be suitable over some narrowband / high latency communications networks.
- A supplicant service is required for operation of 802.1x. For Windows XP SP3, Windows 7 and Windows 8.1, use the Windows-provided "Wired AutoConfig".
- Make sure the authentication service host is reachable from all Mult-IP Gateways in the same farm.
- Provision your Radius server with all Mult-IP Gateway host IPs to be used as Radius clients.

To set up 802.1x authentication for individual functional groups,

1. Log on to the management console with sufficient privileges and expand the **Policies** > **Client Policies** nodes.
2. Right-click a target functional group and select **Authentication** from the context menu to display the main Authentication selection window:



Authentication Method: None



Authentication Method: 802.1X/Radius

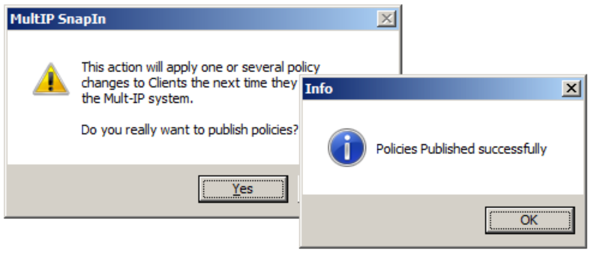
Radius Server:

Radius Secret:

Radius Port: (1 to 65535)

Radius Timeout: (1000 to 30000 ms)

3. As shown, select **802.1x/Radius** from the drop-down list and enter Radius server credentials as described next:
   a) Type the static IP address of the physical machine running the authentication service with embedded Radius Server in the **Radius Server** field.
   b) Click the **Radius Secret** field and type the text string used as a password shared between the Mult-IP Gateways and the Radius server.
   c) Type the port number reserved for communication with the Radius server software.
   d) Click the **Radius Timeout** field and type the amount of time (ranging from 1000 to 30000 milliseconds) allowed for response from the Radius server to an authentication request. Failure to respond within the set timeframe will result in an authentication error message returned to the mobile client.
4. Once you are satisfied with your settings, click **Apply** to save changes and close the window.
5. Again, right-click the target functional group and select **Publish Policies.** Wait for the next confirmation message.



This action will apply one or several policy changes to Clients the next time they the Mult-IP system.

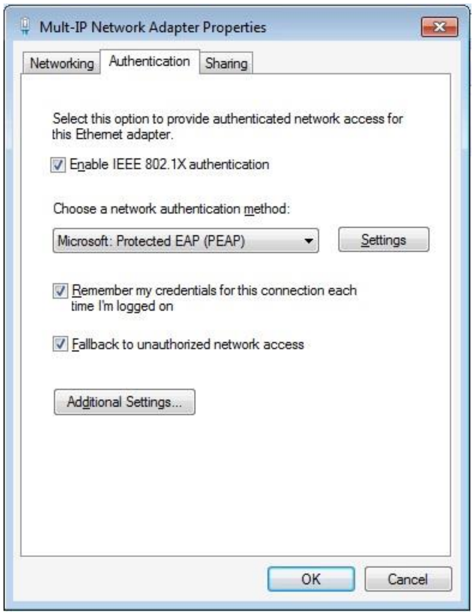
Do you really want to publish policies?

Policies Published successfully

6. Click **Yes** followed by **OK**. The new 802.1x authentication method will be saved as new policies, which will be uploaded to new mobile clients assigned to this functional group or to existing group clients reconnecting to a Mult-IP Gateway using Reset Connection. The new authentication will take effect once supplicant service is enabled, as described next.

To activate 802.1x authentication on the mobile client,

1. With supplicant service running on mobile clients, select the Mult-IP Network Adapter from your list of network connections. As shown next, click the **Authentication** tab and check **Enable IEEE 802.1x authentication**.



Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

2. Select **Microsoft Protected (EAP)** from the authentication method drop-down list.
3. Click **Settings** to display the Protected EAP Properties window and uncheck **Validate Server Certificate.** Validation may interfere with authentication and may need to be de-activated because it may require communication to an external server while authenticating.
4. Click **Configure** and uncheck the **Automatically use my Windows logon…** option and click **OK** to close.
5. Click **OK** twice to close remaining windows.

Extended Support for Single Sign On in 802.1x

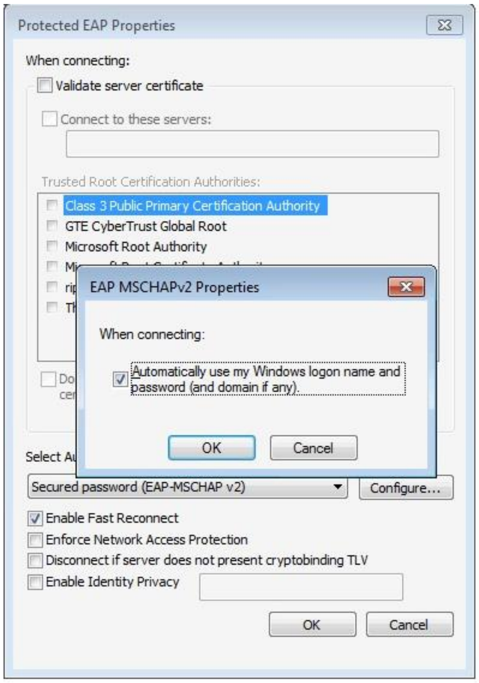
Single Sign-On is a unique policy based mechanism that simplifies user authentication while providing a strong layer for network and service authentication. The streamlined process enables a user to log in once and gains access to multiple resources without being prompted to log in again at each of them.

The mobile client must first join the domain under normal connection and obtain machine credentials. These credentials will be stored on the local machine for authentication purposes. Once Windows is booted up, the client machine will connect to the corporate network using machine-authentication.

With credentials stored on the mobile client, the user employs standard Windows logon to supply domain credentials (username and password) to be validated against a Radius server. Upon successful logon, users are allowed to exchange data with corporate network resources.

To extend support for Single Sign On,

1. Pick up from step 3 in the previous section to display the Protected EAP Properties window.
2. Click **Configure**.



Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

- □ Class 3 Public Primary Certification Authority
- □ GTE CyberTrust Global Root
- □ Microsoft Root Authority

EAP MSCHAPv2 Properties

When connecting:

☑ Automatically use my Windows logon name and password (and domain if any).

Secured password (EAP-MSCHAP v2)

- ☑ Enable Fast Reconnect
- □ Enforce Network Access Protection
- □ Disconnect if server does not present cryptobinding TLV
- □ Enable Identity Privacy

3. As shown, make sure that the **Automatically use my Windows Logon…** option is checked.
4. Click OK twice to close all windows.

Pre-Authentication filters

Pre-Authentication filters allow specific network traffic, authentication traffic in particular, to pass between the client and the gateway, when the client is not yet authenticated by the Mult-IP Gateway. These filters are part of the client policies at the group level and they are processed during the registration steps. The packets are passed as system messages and do not require the Mult-IP channel to be opened. Only packets specified by the filter rules are allowed to be exchanged.

Authentication Rules

The necessary rules can be created from the Authentication Rules manager or imported from an external file, either created by an administrator or provided by Radio IP. Each rule is defined by a unique GUID.

A rule can accept the following parameters:

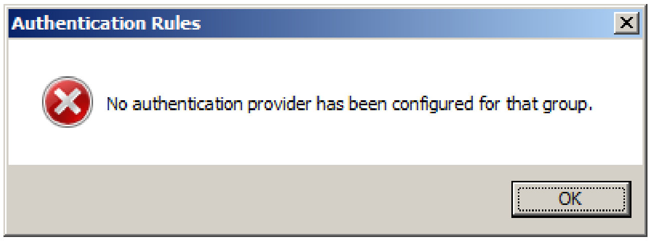
- **IP Address**: if the IP Address is set to **0.0.0.0**, all packets are allowed and this parameter is not used to filter the inbound/outbound traffic.
- **Protocol**: If the protocol is set to **ALL** or *****, any port is allowed and this parameter is not used to filter the inbound/outbound traffic.
- **Start port**: it is the first port of a possible range of ports. If the start port is set to **0**, all ports are allowed and this parameter is not used to filter the inbound/outbound traffic.
- **End port**: it is the end port of a range of ports. When a single port is used by a rule, the end port should be set to 0.
- **Activation flag**: indicates if a rule is active or not. If inactive, the system does not process the rule.
- **Description**: the description is optional and is only used to describe a rule.

Authentication Rules manager

The rules are managed in the Authentication Rules manager. An authentication provider must be configured in order to access the Authentication Rules manager. An authentication provider is one of the authentication methods, such as Radius, 802.1X, etc., chosen for a group authentication policy (Refer to the Authentication section).

Note: It is possible to view and modify the authentication parameters from the Authentication Tab. However, the Authentication option must be used to configure or to change the authentication provider.

If the authentication provider is not configured at the moment of opening the Authentication Rules manager, the following message will be displayed:



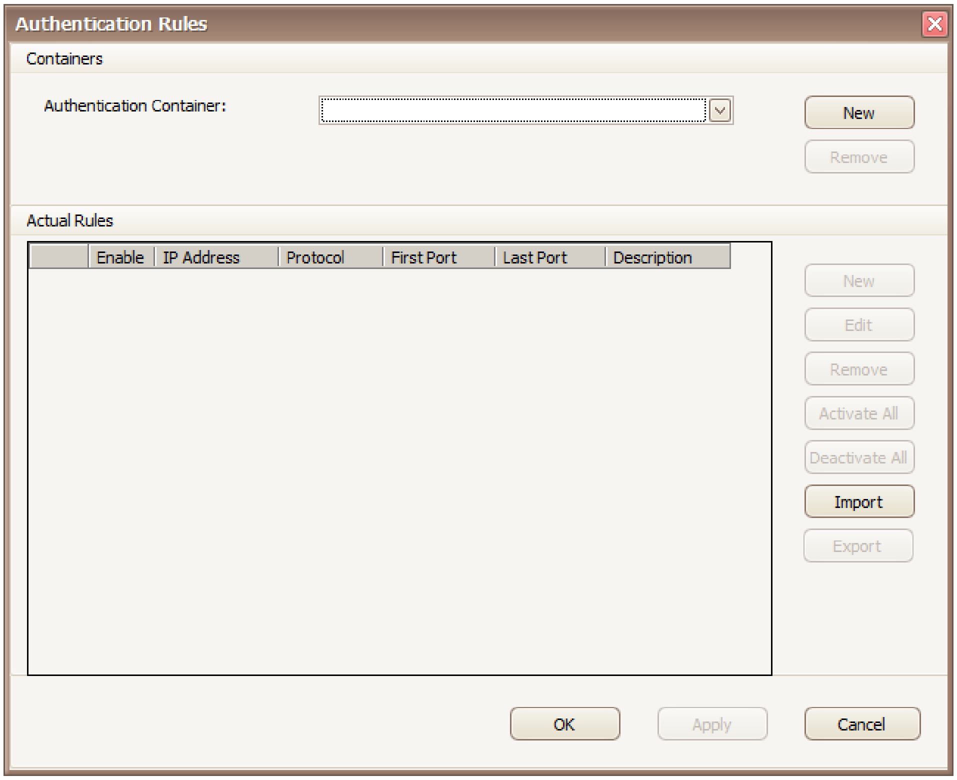
Authentication Rules

No authentication provider has been configured for that group.

The rules can be accessed when configuring client group policies.

The following actions can be performed in the Authentication Rules manager:

- Creating a new container.
- Removing an existing container and all the associated rules.
- Creating a new rule.
- Modifying a rule.
- Removing a rule.
- Activating/Deactivating a rule.
- Activating/Deactivating all rules.
- Importing a set of rules from a comma separated file or text file.
- Exporting configured rules to a comma separated file or text file.

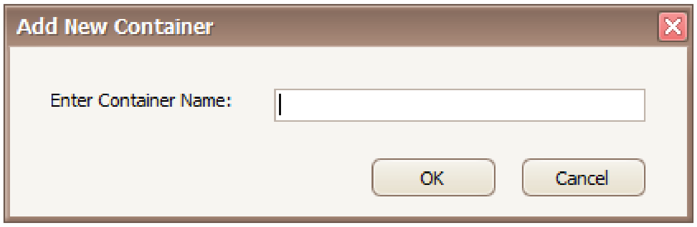


Containers

The rules are grouped into logical sections, called containers. When a packet must get validated by rules, all rules in every container are used. It gets transmitted if it matches one of them.

To create a new container,

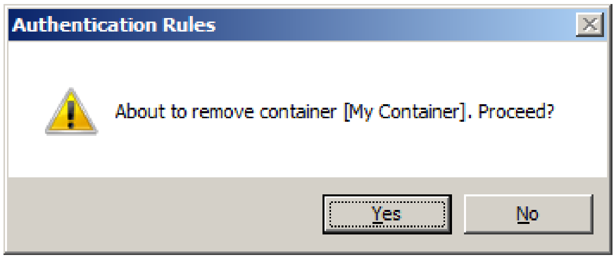
1. Click the **New** button in the **Containers** section of the **Authentication Rules** manager. Enter the container name when the following dialog box is displayed and click **OK**.



2. Click OK to confirm container creation.

To remove a container,

1. Select the container in the container control list and click the **Remove** button in the **Containers** section of the manager. The following confirmation message will be displayed:



About to remove container [My Container]. Proceed?

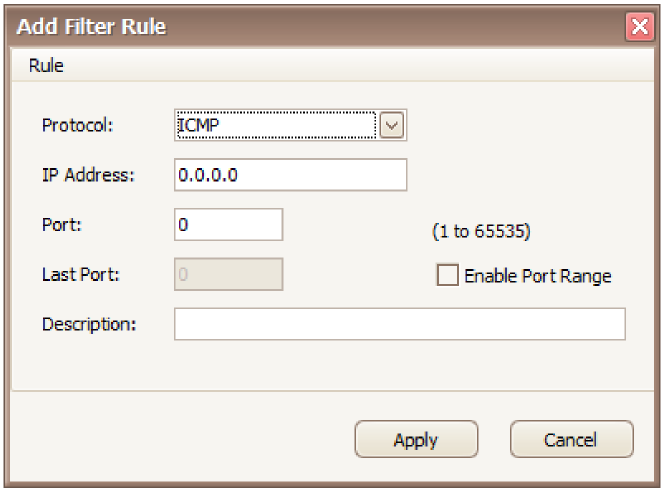
2. Click **Yes** to remove the container or **No** to cancel the operation.

To create a new rule,

1. Click the **New** button in the **Actual Rules** section of the **Authentication Rules** manager.

Note: The creation of a rule is only possible within a container. The **New** button is not enabled if a container was not created.

The following dialog box will be displayed to define the rule:



Protocol: ICMP

IP Address: 0.0.0.0

Port: 0 (1 to 65535)

Last Port: 0 □ Enable Port Range

Description:

This dialog box allows to select:

- A **protocol: e**nter **ALL** or ***** for the rule to accept all protocols.
- An **IP address:** enter **0.0.0.0** for the rule to accept all IP Addresses.
- A **port** or a **range of ports**: accepts values from 1 to 65535. To be able to enter a range of ports, click the **Enable Port Range** checkbox to enable the **Last Port** field.
- A **description:** the description is optional and only used to describe a rule.

2. Click the **Apply** button to save the rule.

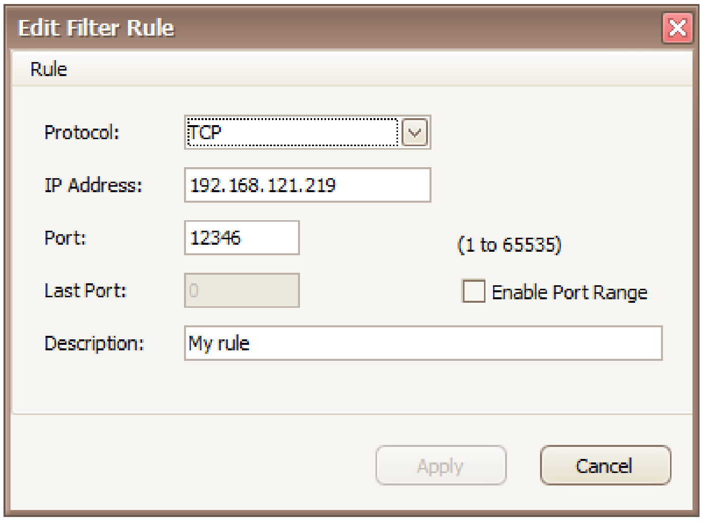
The following table lists some example protocols and ports that can be used for the user authentication:

Name	Protocol	Port
Active Directory		
Domain Name System (DNS)	TCP/UDP	53
Lightweight Directory Access Protocol (LDAP)	TCP/UDP	389
Microsoft EPMAP (End Point Mapper), also known as DCE/RPC Locator service, used to remotely manage services including DHCP server, DNS server and WINS. Also used by DCOM	TCP/UDP	135
NetBIOS Name Service	TCP/UDP	137
NetBIOS Datagram Service	TCP/UDP	138
NetBIOS Session Service	TCP/UDP	139

Name	Protocol	Port
Microsoft-DS Active Directory, Windows shares	TCP	445
Kerberos—authentication system	TCP/UDP	88
Dynamic	TCP/UDP	1025-5000 49152-65535
ICMP		
Other		
Domain Name System (DNS) RNDC Service	TCP/UDP	953
Multicast DNS (mDNS)	UDP	5353
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)	TCP/UDP	636
Microsoft Global Catalog (LDAP service which contains data from Active Directory forests)	TCP/UDP	3268
Microsoft Global Catalog over SSL (similar to port 3268, LDAP over SSL)	TCP/UDP	3269
Kerberos Change/Set password	TCP/UDP	464

To modify an existing rule,

1. Select the rule to be modified and click the **Edit** button. The following dialog box will be displayed:



Edit Filter Rule

Rule

Protocol: TCP

IP Address: 192.168.121.219

Port: 12346 (1 to 65535)

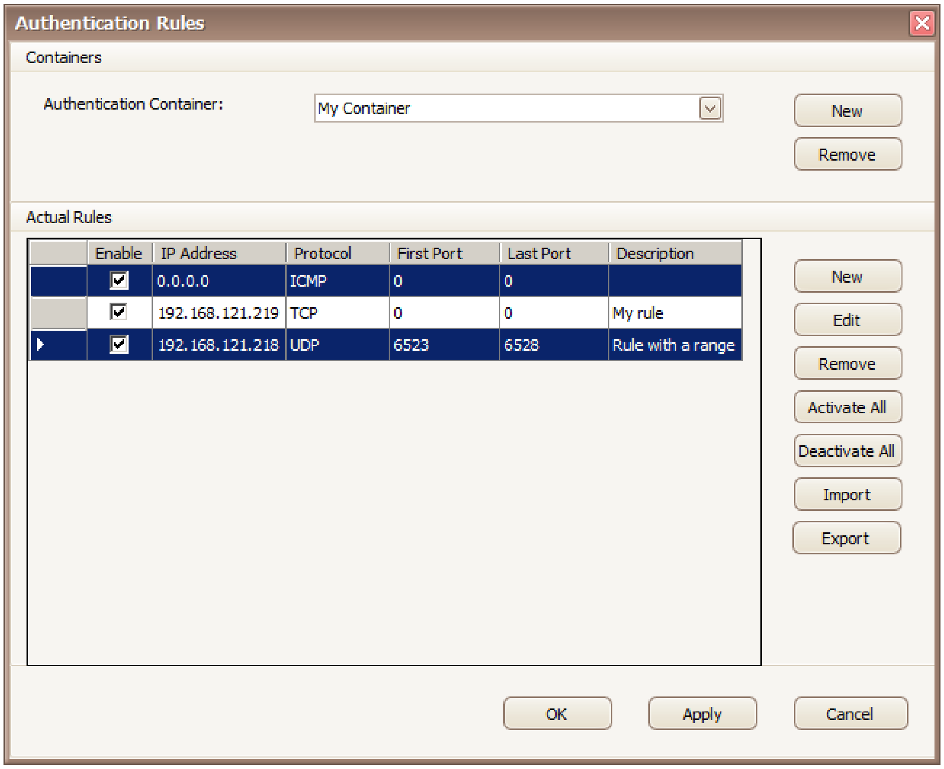
Last Port: 0 □ Enable Port Range

Description: My rule

2. Modify the rule and click the **Apply** button. The **Apply** button will only be enabled if a field has been modified. Click **Cancel** to cancel the operation.

To remove a rule or a selection of rules,

1. Select the rule or the rules (hold the **Ctrl** key to select several rules) to be removed as shown below and click the **Remove** button.



Authentication Rules

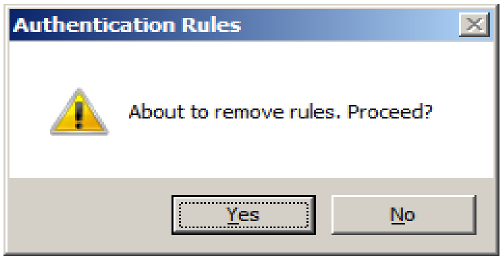
Containers

Authentication Container: My Container

Actual Rules

	Enable	IP Address	Protocol	First Port	Last Port	Description
	☑	0.0.0.0	ICMP	0	0	
	☑	192.168.121.219	TCP	0	0	My rule
▶	☑	192.168.121.218	UDP	6523	6528	Rule with a range

The following message will ask to confirm the deletion:



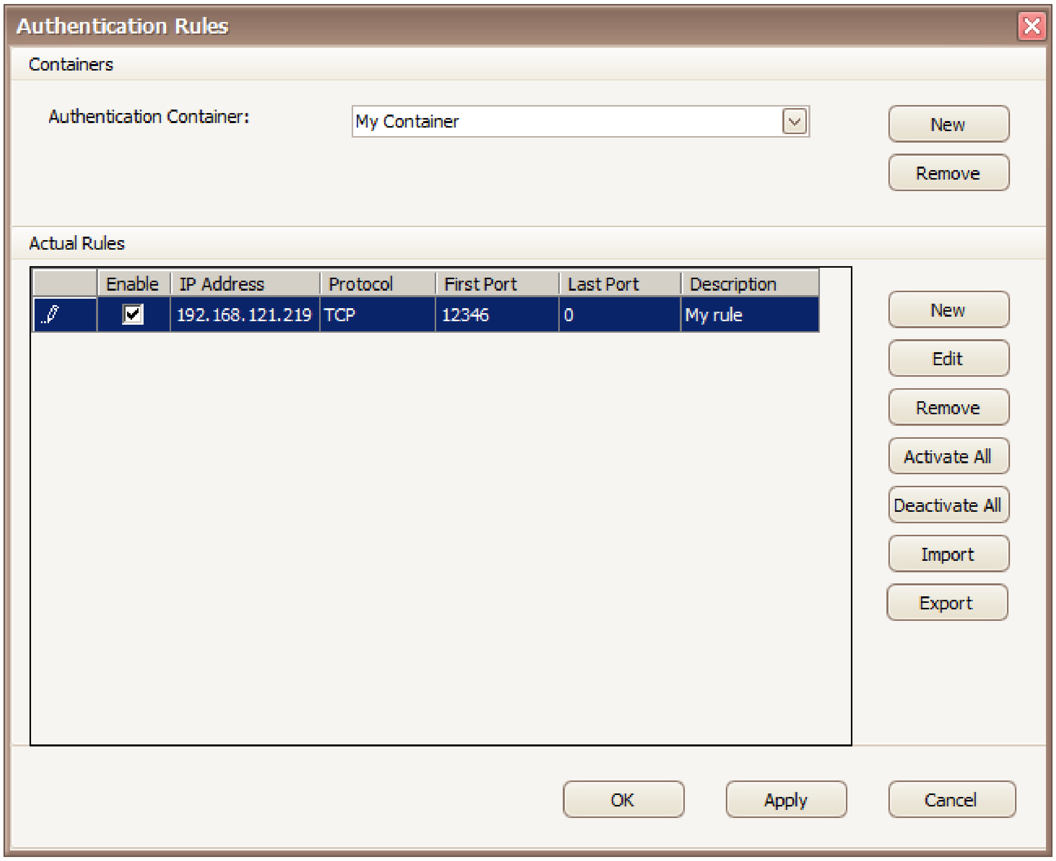
Authentication Rules

About to remove rules. Proceed?

2. Click **Yes** to remove the rule or **No** to cancel the operation.

To activate or deactivate a rule,

To activate or deactivate a rule, click the **Enable** checkbox in the **Actual Rules** section. The figure below shows an activated rule:



Authentication Rules

Containers

Authentication Container: My Container

Actual Rules

	Enable	IP Address	Protocol	First Port	Last Port	Description
	☑	192.168.121.219	TCP	12346	0	My rule

To activate or to deactivate all rules,

Click the **Activate All** or **Deactivate All** button.

Importing a set of rules from a file

This feature is used to import a set of rules from a file. Rules can be created in a file by an administrator or can be imported from a previously exported file. A file may contains rules for different containers.

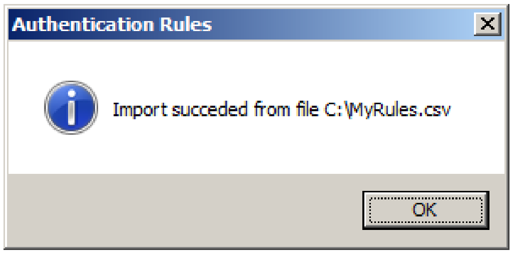
The following is an example of a file format:

```
####
#### Format is
#### Container Rule Name, IP Address, Protocol, First Port, Last Port,
Activated, Description
#### Last Port is 0 when port range is not used
#### Activated must be true or false
#### All lines starting with # are ignored
####
```

```
ADrule, 172.27.0.10, TCP, 53, 0, true, DNS
ADrule, 172.27.0.10, UDP, 53, 0, true, DNS
EntrustSSM, 172.27.0.139, TCP, 8445, 0, true, Allow Self Service Module
MyContainer, 172.27.0.140, ALL, 8445, 0, true, Allow Self Service
Module
MyContainer, 172.27.0.140, TCP, 9000, 9010, true, Allow Self Service
Module
```

Note: A line starting with # is ignored.

When a file is imported successfully, the following message is displayed and the Authentication Rules manager is updated with the new containers and rules:



Import succeded from file C:\MyRules.csv

Exporting a set of rules to a comma separated file

This feature is used to export the current set of rules to a file. The file generated will be in the following format:

```
#### Export file generation information
####
#### Generated On : COMPUTER
#### Generated By : USER
####
#### Generate Date : 05/09/2014
####
#### Server Context : CONTEXT
####
#### Rule Version : 1
####
#### Format is
#### Container Rule Name, IP Address, Protocol, First Port, Last Port,
Activated, Description
```

```
#### Last Port is 0 when port range is not used
#### Activated must be true or false
#### All lines starting with # are ignored
####
ADrule, 172.27.0.10, TCP, 53, 0, true, DNS
ADrule, 172.27.0.10, UDP, 53, 0, true, DNS
ADrule, 172.27.0.10, TCP, 88, 0, true, Kerberos-authentication system
ADrule, 172.27.0.10, UDP, 88, 0, true, Kerberos-authentication system
ADrule, 172.27.0.10, TCP, 135, 0, true, Microsoft EPMAP (End Point
Mapper)
ADrule, 172.27.0.10, UDP, 135, 0, true, Microsoft EPMAP (End Point
Mapper)
ADrule, 172.27.0.10, TCP, 137, 0, true, NetBIOS Name Service
ADrule, 172.27.0.10, UDP, 137, 0, true, NetBIOS Name Service
ADrule, 172.27.0.10, TCP, 138, 0, true, NetBIOS Datagram Service
ADrule, 172.27.0.10, UDP, 138, 0, true, NetBIOS Datagram Service
ADrule, 172.27.0.10, TCP, 139, 0, true, NetBIOS Session Service
ADrule, 172.27.0.10, UDP, 139, 0, true, NetBIOS Session Service
ADrule, 172.27.0.10, TCP, 389, 0, true, Lightweight Directory Access
Protocol (LDAP)
ADrule, 172.27.0.10, UDP, 389, 0, true, Lightweight Directory Access
Protocol (LDAP)
ADrule, 172.27.0.10, TCP, 445, 0, true, Microsoft-DS Active Directory
ADrule, 172.27.0.10, UDP, 445, 0, true, Microsoft-DS Active Directory
ADrule, 172.27.0.10, ICMP, 0, 0, true, Internet Control Message
Protocol
ADrule, 172.27.0.10, TCP, 464, 0, true, allow464TCP
ADrule, 172.27.0.10, UDP, 464, 0, true, allow464UDP
ADrule, 172.27.0.10, TCP, 636, 0, true, allow636TCP
ADrule, 172.27.0.10, TCP, 1024, 5000, true, allowdynamicTCP
ADrule, 172.27.0.10, UDP, 1024, 5000, true, allowdynamicUDP
ADrule, 172.27.0.10, TCP, 49152, 65535, true, allowdynamicTCP
ADrule, 172.27.0.10, UDP, 49152, 65535, true, allowdynamicUDP
EntrustSSM, 172.27.0.139, TCP, 8445, 0, true, Allow Self Service Module
MyContainer, 172.27.0.140, ALL, 8445, 0, true, Allow Self Service
Module
MyContainer, 172.27.0.140, TCP, 9000, 9010, true, Allow Self Service
Module
```

Applying Updates through Remote Update

Radio IP occasionally releases updates to its Mult-IP Mobile VPN solution consisting of enhancements or issue fixes. Through Remote Update, the system administrator typically mounts an update of the latest client software on the gateway platform and publishes that update to some or all functional groups. The Mult-IP Client software is then pushed to mobile devices, alleviating the need for a fleet recall. Naturally, the amount of time required to update an entire fleet depends on many factors, which ultimately break down to the following paradigm:

● Remote Update file size ● network traffic ● wireless driver performance

Update packages are transferred to clients over Pipe 3. Larger files will be uploaded in less time in low traffic situations over broadband networks (such as late generation cellular or Wi-Fi). Look for step 6 of the upcoming procedure to limit the number of concurrent downloads and mitigate performance issues raised, for instance, by a large-scale update or application data also assigned to Pipe 3.

Getting Started

The task of readying a file for remote update is performed on a Mult-IP Gateway using Microsoft PowerShell task automation framework, consisting of a command-line interface and associated scripting language built on top of, and integrated with the .NET Framework.

As a prerequisite, log on to the Mult-IP Gateway where you plan to conduct most of your work and enable PowerShell. Refer to the Windows help or query Microsoft online resources for assistance.

Registering a Remote Update Package

This section shows you how to register x86 and x64 Mult-IP Client update packages on the Mult-IP Gateway. This section assumes that you have obtained the `*.msi` client update files (both x86 and x64) from Radio IP and that you have saved those files in a known location on the gateway machine where you plan to register the update. Note that you will have to provide this path later in the process.

Upgrade packages (“Mult-IP.msi”) are used to pass from one official software version to another. For example they would allow a client to upgrade from 3.9.0 to 3.9.1. They are identified in PowerShell and in the console with 3 numbers.

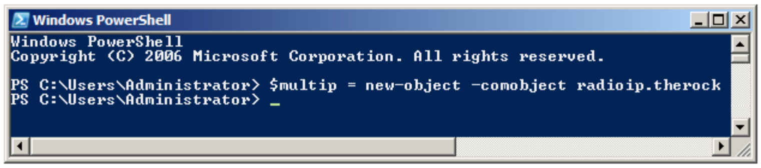
Patch packages (“<product><baseline>To<patchID>.msp”) are used for minor modifications over analready installed baseline. For example the patch 3.9.1.3572 requires the baseline 3.9.1 to be already installed. It does not matter if 3.9.1 was already patched. Those files are identified with 4 numbers in PowerShell and in the console.

Note: You must reapply the remote update package registration process after a Mult-IP Gateway upgrade.

To register a remote update package,

1. Log on to the gateway machine where the update files are stored and start PowerShell.
2. Type the following command followed by <Enter> to connect the CLI to the Mult-IP API.

```
$multip = new-object –comobject radioip.therock
```



```
Windows PowerShell
Copyright (C) 2006 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> $multip = new-object -comobject radioip.therock
PS C:\Users\Administrator> _
```

.

3. Issue the following command to connect and authenticate to the Mult-IP API.

    `$multip.OpenSession("username", "password", $null)`

where `"username"` and `"password"` refer to the SuperUser credentials supplied during initial logon to the management console.

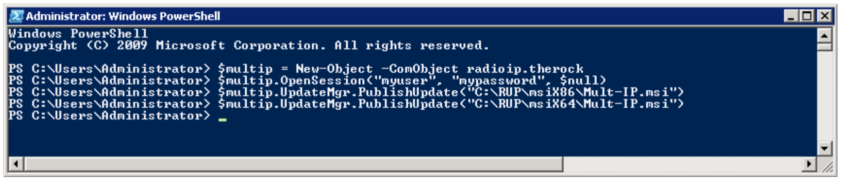
4. Issue the following command upon successful login to the Mult-IP API:

    `$multip.updatemgr.publishupdate(“full path”)`

where `"full path"` points to the source location and filename, such as in the following example:

for an x86 update: `C:\RUP\x86\Mult-IP.msi`
for an x64 update: `C:\RUP\x64\Mult-IP.msi`

This will copy the x86 or x64 update msi files from a source location to the Mult-IP Gateway's update folder (`C:\Program Files\RadioIP\Data\Updates`).



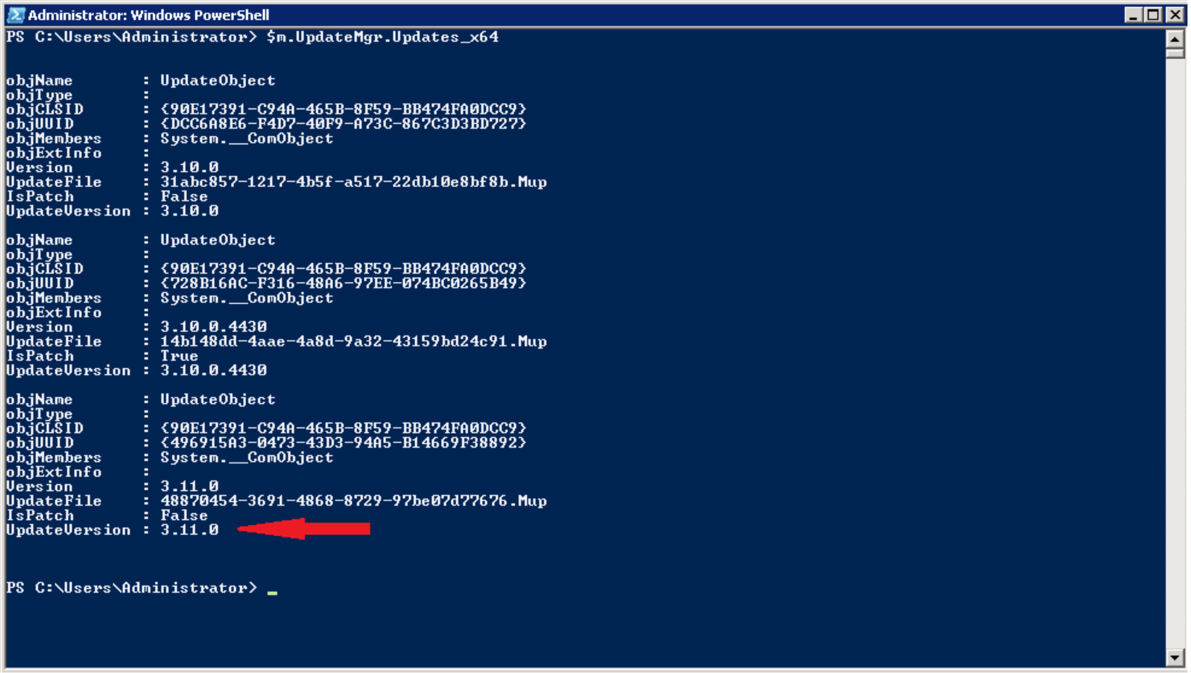
```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> $multip = New-Object -ComObject radioip.therock
PS C:\Users\Administrator> $multip.OpenSession("myuser", "mypassword", $null)
PS C:\Users\Administrator> $multip.UpdateMgr.PublishUpdate("C:\RUP\msiX86\Mult-IP.msi")
PS C:\Users\Administrator> $multip.UpdateMgr.PublishUpdate("C:\RUP\msiX64\Mult-IP.msi")
PS C:\Users\Administrator> _
```

Notes:

- Update files are synchronized to all load-balancing gateways. This process, which may span several minutes, requires that each gateway downloads files to its respective update folder.
- PowerShell may not handle extended paths names so keep source path as short as possible.
- Do not rename *`.msi` to prevent files from being unrecognized by the Mult-IP Client update utility.

5. Run the following command to retrieve the list of all available updates:
    a) For x86 systems, type: `$multip.updatemgr.updates_x32`
    b) For x64 systems, type: `$multip.updatemgr.updates_x64`



```
PS C:\Users\Administrator> $m.UpdateMgr.Updates_x64


objName       : UpdateObject
objType       :
objCLSID      : {90E17391-C94A-465B-8F59-BB474FA0DCC9}
objUUID       : {DCC6A8E6-F4D7-40F9-A73C-867C3D3BD727}
objMembers    : System.__ComObject
objExtInfo    :
Version       : 3.10.0
UpdateFile    : 31abc857-1217-4b5f-a517-22db10e8bf8b.Mup
IsPatch       : False
UpdateVersion : 3.10.0

objName       : UpdateObject
objType       :
objCLSID      : {90E17391-C94A-465B-8F59-BB474FA0DCC9}
objUUID       : {728B16AC-F316-48A6-97EE-074BC0265B49}
objMembers    : System.__ComObject
objExtInfo    :
Version       : 3.10.0.4430
UpdateFile    : 14b148dd-4aae-4a8d-9a32-43159bd24c91.Mup
IsPatch       : True
UpdateVersion : 3.10.0.4430

objName       : UpdateObject
objType       :
objCLSID      : {90E17391-C94A-465B-8F59-BB474FA0DCC9}
objUUID       : {496915A3-0473-43D3-94A5-B14669F38892}
objMembers    : System.__ComObject
objExtInfo    :
Version       : 3.11.0
UpdateFile    : 48870454-3691-4868-8729-97be07d77676.Mup
IsPatch       : False
UpdateVersion : 3.11.0



PS C:\Users\Administrator> _
```

6. As an option, you may run the following command to set the number of concurrent downloads.

   ```
   $multip.updatemgr.concurrentclients = x
   ```

   where “x” sets the number of concurrent downloads.

7. To acknowledge the value set above, run:

   ```
   $multip.updatemgr.ConcurrentClients
   ```

Use this setting to limit the impact on download speed of a large number of mobile clients allowed to download an update concurrently (commonly known as “throttling”). When setting the number of concurrent downloads, keep in mind that remote updates are transported over Pipe 3 which may also be shared with application data depending on filter rule definitions.

Note: The default value of “0” sets the number of simultaneous downloads to unlimited.

8. In our example, x86 and x64 files targeted at the same version number are registered and synchronized across all gateways in a load-balancing environment. Take note of the exact version number in the UpdateVersionfield (highlighted by the red arrow), then you may close the PowerShell window.

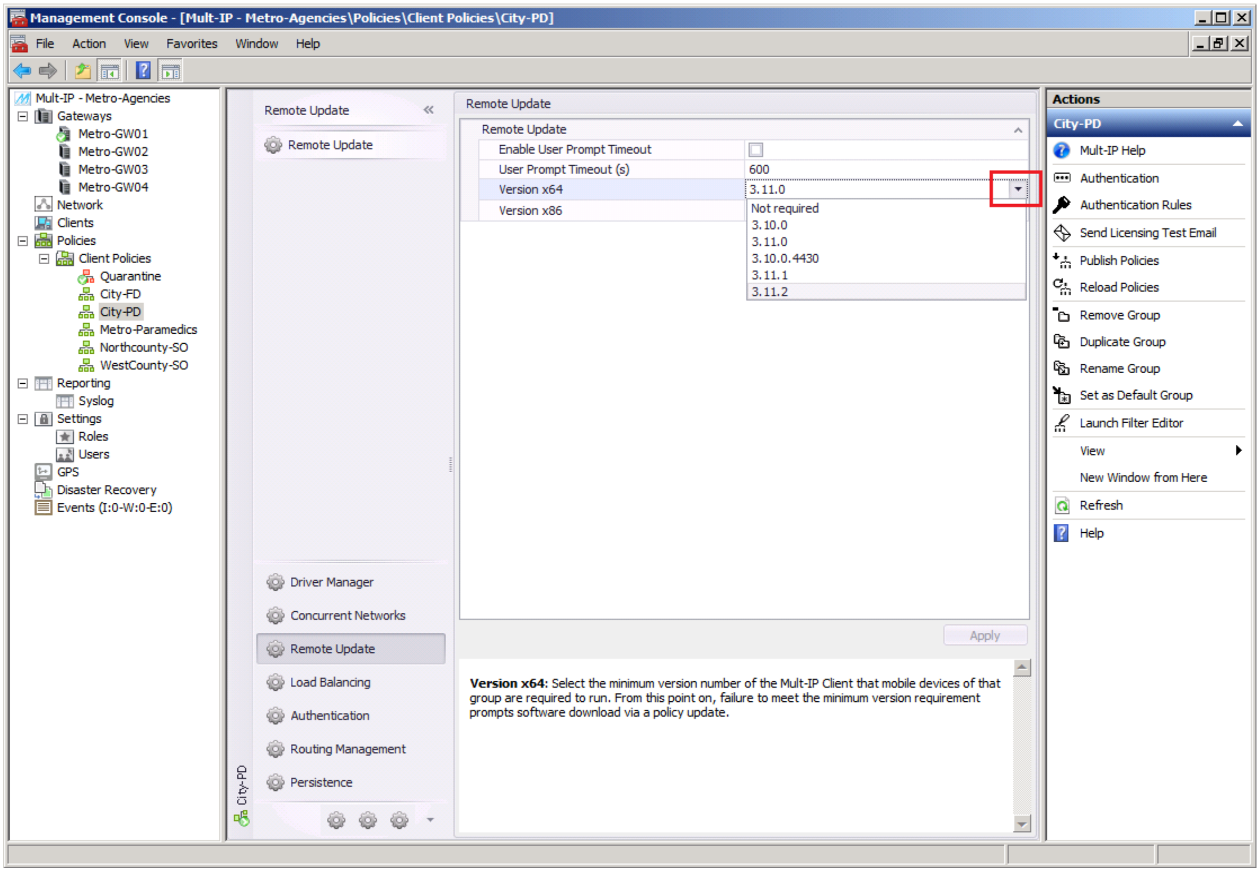
Publishing Updates

With update packages ready for download, group policies must be published with minimum version information. Upon registration to the Mult-IP network, clients will take notice of the new policy and start downloading the update software.

Notice to Active Directory users: Be advised that any change to the default behavior of the **Software Restriction** policy, and implementation of such policy in a Group Policy Object (GPO) is likely to prevent Mult-IP remote update package executables (for example *.exe, *.msi files) from running on mobile clients, thus blocking the remote update process. Specifically, avoid setting the **Software Restriction** policy as the default rule in Security Levels with rule set to **Disallowed**.

To publish updates,

1. In the management console, click the functional group whose clients you wish to update, then click the **RemoteUpdate** tab.



Management Console - [Mult-IP - Metro-Agencies\Policies\Client Policies\City-PD]

Remote Update	
Enable User Prompt Timeout	□
User Prompt Timeout (s)	600
Version x64	3.11.0
Version x86	

Not required
3.10.0
3.11.0
3.10.0.4430
3.11.1
3.11.2

Version x64: Select the minimum version number of the Mult-IP Client that mobile devices of that group are required to run. From this point on, failure to meet the minimum version requirement prompts software download via a policy update.

Click both **Version x64** and **Version x86** fields and select the minimum version number of the Mult-IP Client that mobile devices of that group are required to run. From this point on, failure to meet the minimum version requirement prompts software download via a policy update. Pay particular attention to this step as your gateway may store multiple update packages over time.

2. The user prompt timeout option defines a time limit for the user to accept Mult-IP client update installation when prompted for a new version availability. Check the **Enable User Prompt Timeout** and enter the time (in seconds) into the **User Prompt Timeout** box if you want to enable this feature:

The Mult-IP Client needs to be in version 3.10 to support this feature.

Note: The **User Prompt Timeout** feature is disabled by default.

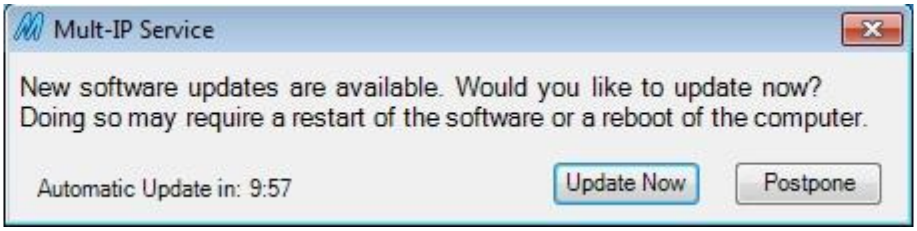
When the **User Prompt Timeout** option is enabled and the timer value is set to 0, the update is performed without prompting the user.

3. Click **Apply** when done.
4. Right-click the group and select **Publish Policies** from the context menu to inform the system of the minimum version required. Repeat this step for all groups whose clients you wish to update.

Once policies have been published, clients of the target functional group(s) **not meeting the minimum software version** will be remotely updated as soon as they reconnect to the gateway by way of a Reset Connection or simply through a new session registration.

The notion of minimum version comes handy in a large organization in which some or all clients of a given group may not require the latest update (or meet hardware or OS requirements). In such a case, allowing a version number lower than that of the available update package would allow them to bypass the update process until that number is manually changed. The download and installation of a client update requires a confirmation and a reboot from the end-user.

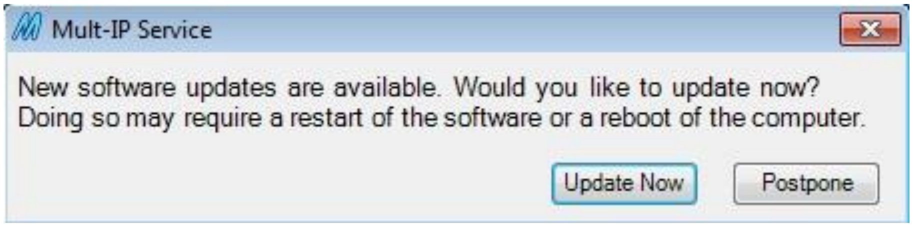
On a Mult-IP client, when the **User Prompt Timeout** feature is activated and the timer is not set to 0, the remote update process will prompt a dialog box indicating the time limit for the user to accept or postpone the update. If the user does not respond before the timeout, the update is performed. If **Postpone** is selected, the user will be prompted later again:



New software updates are available. Would you like to update now?
Doing so may require a restart of the software or a reboot of the computer.

Automatic Update in: 9:57

If the client is running a version up to 3.9 inclusive, or if the feature is not enabled on the gateway, then the user is prompted a dialog without any time limit. If **Postpone** is selected, the user will be prompted later again:



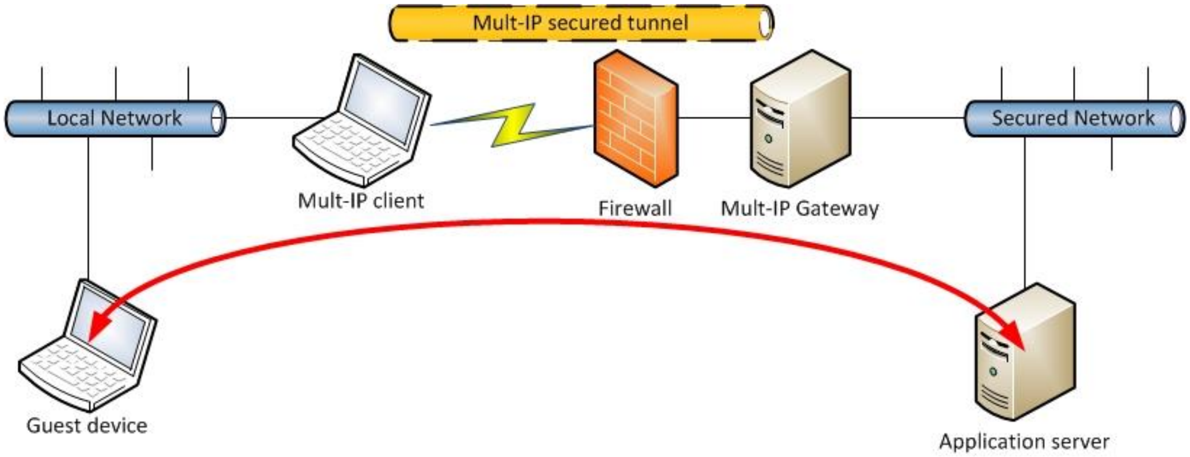
New software updates are available. Would you like to update now?
Doing so may require a restart of the software or a reboot of the computer.

If you wish to control which clients to upgrade, you may dedicate a single functional group to the task of processing remote updates. For example, you could temporarily set this group as default and automatically allow updates to take place as clients register. This practice would contain any mistake made during update registration or publishing to a controlled group, thus limiting the impact on large production environments.

Note: For example, to allow clients running the version 3.8.6 to update to version to 3.10.0 and apply the patch 3.10.0.4430, you would need to register both the 3.10.0 baseline and the patch 3.10.0.4430 in PowerShell. The entry of the version 3.10.0.4430 into the Remote Update field of this group in the console will cause the clients with 3.10.0 to download and apply the patch. The clients with a version smaller than 3.10.0 will first download the 3.10.0 baseline, apply it, reboot and then download the 3.10.0.4430 patch, apply it over the 3.10.0 and reboot a second time.

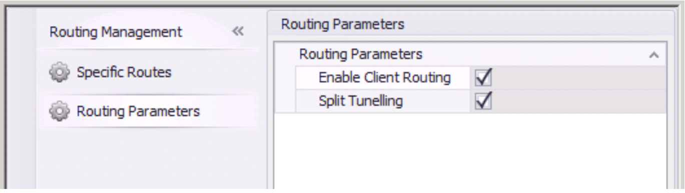
Client routing

A Mult-IP client may be used as a router device for other devices on the local Mult-IP client network, and give them access to the Secured Network resources through the Mult-IP tunnel:



To enable the client routing feature,

1. Select the functional group whose clients will be allowed to take advantage of the traffic-forwarding feature and select the **Routing Management** tab in the group workspace.
2. Open the Routing Parameters section, check the “Enable Client Routing” checkbox:



Enable Client Routing	☑
Split Tunelling	☑

3. Click **Apply**.
4. Perform a new **Publish Policies** when ready.

Split Tunneling

Split tunneling is a networking feature that allows functional group clients to bypass the Mult-IP Mobile VPN and access the connected local area networks while still relying on Mult-IP for mission-critical corporate applications and services, both of which are carried on the same physical connections.

Consider the case of a user accessing the corporate network through Mult-IP using his home network. The user with split tunneling enabled is therefore able to connect to a file server, database server, mail server and other corporate network resources through the Mult-IP Mobile VPN connection. When the user accesses the Internet for leisure or research, the connection request originates from the web browser directly to the home gateway.

Considerations

Review these guidelines before enabling split tunneling, especially in mission-critical environments:

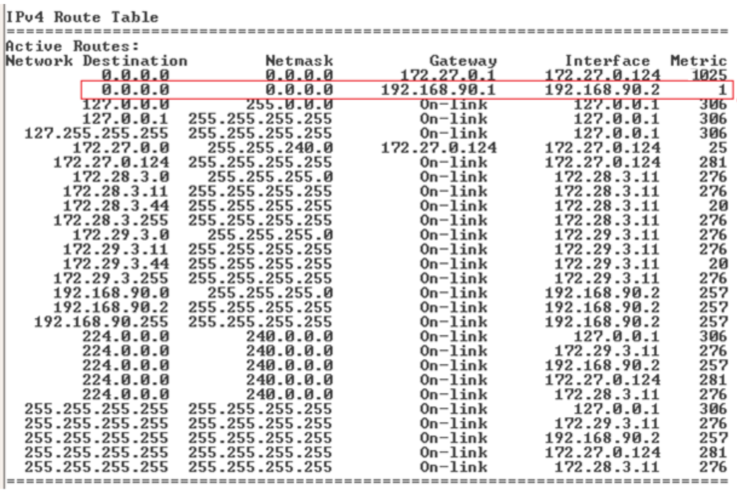
- One advantage of using split tunneling is that it alleviates bottlenecks and conserves bandwidth as local and Internet traffic does not have to pass through the Mult-IP gateways.
- Another advantage is in the case where a user works on partner sites and needs access to resources on both partner and corporate networks throughout the day. Split tunneling prevents the user from having to toggle constantly connections.
- Be aware of increased vulnerability: as packets not related to your mission-critical application travel outside Mult-IP, split tunneling typically bypasses the gateway security provided by filter rules.

Enabling the Split Tunneling feature

Split tunneling is mainly used to relieve Mult-IP Gateways from traffic that can otherwise transit over public networks. Enabling this feature is a straightforward process which will have you provision group policy with as many routes as are needed to access specific, work-related corporate resources.

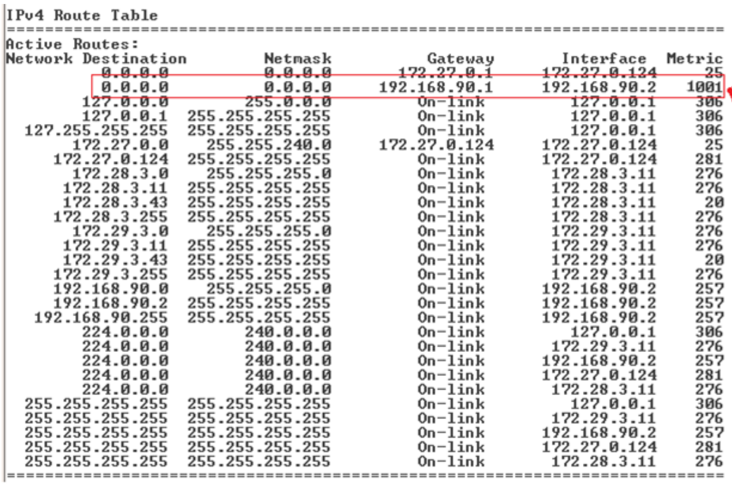
When considering adding split tunneling functionality to your organization, always keep in mind that:

- Without split tunneling, all packets go through the VPN tunnel. Therefore, there is no need to define specific routes to LAN-based application servers.
- With split tunneling enabled, the Mult-IP default gateway metric increase by 1000. This de-prioritization demonstrated in the following client routing table sample allows all packets to bypass the VPN tunnel except for those targeting specific routes added to reach application servers.
- Configuration is saved in system storage and pushed to clients as a group policy update. This process is completely transparent to the end-user.



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       172.27.0.1     172.27.0.124   1025
          0.0.0.0          0.0.0.0     192.168.90.1     192.168.90.2      1
        127.0.0.0        255.0.0.0          On-link        127.0.0.1    306
        127.0.0.1  255.255.255.255          On-link        127.0.0.1    306
  127.255.255.255  255.255.255.255          On-link        127.0.0.1    306
       172.27.0.0    255.255.240.0     172.27.0.124     172.27.0.124     25
     172.27.0.124  255.255.255.255          On-link     172.27.0.124    281
       172.28.3.0    255.255.255.0          On-link      172.28.3.11    276
      172.28.3.11  255.255.255.255          On-link      172.28.3.11    276
      172.28.3.44  255.255.255.255          On-link      172.28.3.11     20
     172.28.3.255  255.255.255.255          On-link      172.28.3.11    276
       172.29.3.0    255.255.255.0          On-link      172.29.3.11    276
      172.29.3.11  255.255.255.255          On-link      172.29.3.11    276
      172.29.3.44  255.255.255.255          On-link      172.29.3.11     20
     172.29.3.255  255.255.255.255          On-link      172.29.3.11    276
     192.168.90.0    255.255.255.0          On-link     192.168.90.2    257
     192.168.90.2  255.255.255.255          On-link     192.168.90.2    257
   192.168.90.255  255.255.255.255          On-link     192.168.90.2    257
        224.0.0.0        240.0.0.0          On-link        127.0.0.1    306
        224.0.0.0        240.0.0.0          On-link      172.29.3.11    276
        224.0.0.0        240.0.0.0          On-link     192.168.90.2    257
        224.0.0.0        240.0.0.0          On-link     172.27.0.124    281
        224.0.0.0        240.0.0.0          On-link      172.28.3.11    276
  255.255.255.255  255.255.255.255          On-link        127.0.0.1    306
  255.255.255.255  255.255.255.255          On-link      172.29.3.11    276
  255.255.255.255  255.255.255.255          On-link     192.168.90.2    257
  255.255.255.255  255.255.255.255          On-link     172.27.0.124    281
  255.255.255.255  255.255.255.255          On-link      172.28.3.11    276
===========================================================================
```

With **Split tunneling disabled**, Mult-IP is set as the default gateway (route with with the highest priority).

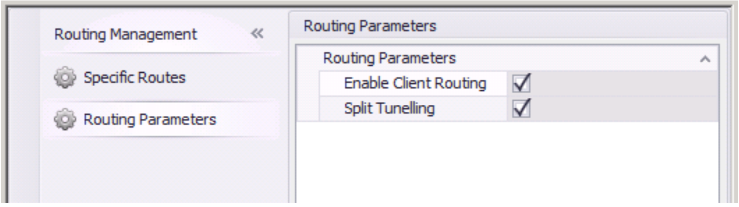


```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       172.27.0.1     172.27.0.124     25
          0.0.0.0          0.0.0.0     192.168.90.1     192.168.90.2   1001
        127.0.0.0        255.0.0.0          On-link        127.0.0.1    306
        127.0.0.1  255.255.255.255          On-link        127.0.0.1    306
  127.255.255.255  255.255.255.255          On-link        127.0.0.1    306
       172.27.0.0    255.255.240.0     172.27.0.124     172.27.0.124     25
     172.27.0.124  255.255.255.255          On-link     172.27.0.124    281
       172.28.3.0    255.255.255.0          On-link      172.28.3.11    276
      172.28.3.11  255.255.255.255          On-link      172.28.3.11    276
      172.28.3.43  255.255.255.255          On-link      172.28.3.11     20
     172.28.3.255  255.255.255.255          On-link      172.28.3.11    276
       172.29.3.0    255.255.255.0          On-link      172.29.3.11    276
      172.29.3.11  255.255.255.255          On-link      172.29.3.11    276
      172.29.3.43  255.255.255.255          On-link      172.29.3.11     20
     172.29.3.255  255.255.255.255          On-link      172.29.3.11    276
     192.168.90.0    255.255.255.0          On-link     192.168.90.2    257
     192.168.90.2  255.255.255.255          On-link     192.168.90.2    257
   192.168.90.255  255.255.255.255          On-link     192.168.90.2    257
        224.0.0.0        240.0.0.0          On-link        127.0.0.1    306
        224.0.0.0        240.0.0.0          On-link      172.29.3.11    276
        224.0.0.0        240.0.0.0          On-link     192.168.90.2    257
        224.0.0.0        240.0.0.0          On-link     172.27.0.124    281
        224.0.0.0        240.0.0.0          On-link      172.28.3.11    276
  255.255.255.255  255.255.255.255          On-link        127.0.0.1    306
  255.255.255.255  255.255.255.255          On-link      172.29.3.11    276
  255.255.255.255  255.255.255.255          On-link     192.168.90.2    257
  255.255.255.255  255.255.255.255          On-link     172.27.0.124    281
  255.255.255.255  255.255.255.255          On-link      172.28.3.11    276
===========================================================================
```

With **Split tunneling** enabled, all routes are prioritized ahead of Mult-IP's default gateway whose metric is increased by 1000.

To enable split tunneling,

5. Select the functional group whose clients will be allowed to take advantage of split tunneling and select the **Routing Management** tab in the group workspace.



Routing Parameters

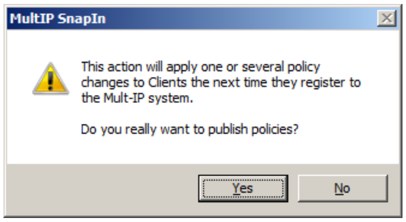
Enable Client Routing	☑
Split Tunelling	☑

6. As shown, check the **Split Tunneling** check box and apply to enable the feature.

7. Open the Specific Routes section and specify the **Destination IP** and **Netmask** for as many routes as are needed to reach corporate resources while Split Tunneling is in use. You may specify an entire segment or type the IP address which points to a specific network resource (such as an application server) whose access should be secured through Mult-IP. Choosing the latter will require you to define specific routes for each network resource. Once you are satisfied with the supplied addresses, click **Apply**.

Note: You can add any number of specific routes. However, they will only apply while Split tunneling is enabled.

8. Right-click the target functional group and select **Publish Policies** from the context menu. Wait for the following confirmation dialogue.



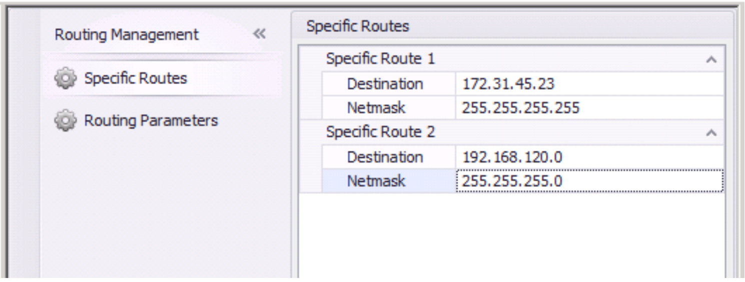
MultIP SnapIn

This action will apply one or several policy changes to Clients the next time they register to the Mult-IP system.

Do you really want to publish policies?

9. Click **Yes** to publish the new route. The policy update will be downloaded and take effect on clients assigned to this group or clients reconnecting through the Reset Connection command. In doing so, the newly defined route will be added to the local machine's routing table, carrying the lowest metric. As indicated earlier, make a habit of specifying machine-specific IP addresses to facilitate destination resolution. See About IP Routing for more on routing tables.

Once policies are published, a blank **SpecificRoute** parameter is added to the **SpecifcParams** workspace.



Specific Route 1

Destination	172.31.45.23
Netmask	255.255.255.255

Specific Route 2

Destination	192.168.120.0
Netmask	255.255.255.0

10. Use the new address entry fields to define an additional route to corporate resources.
11. Perform a new **Publish Policies** when ready.
12. Repeat the process of specifying specific routes in order to account for any foreseeable route that may be required by any one member of the target group.

Managing Connection Persistence

Persistence refers to a gateway's ability to monitor periodically registered mobile clients at the functional group level. On the one hand, gateways check for in-coverage status and, if needed, will automatically allow clients back on the network after a break in communication has occurred (useful when a vehicle expectedly loses signal while crossing an underground tunnel). On the other hand, gateways check for TCP socket activity, closing connections if none is reported.

Mult-IP supports connection persistence at the following activity levels: session and application.

- **Session persistence**

  Session persistence ensures that clients will automatically resume their active work session (with no registration required) as long as they experience a communication failure lasting no more than a configurable duration. Consequently, as an additional security measure, clients reconnecting outside the preset duration will be forced to register and optionally authenticate to the corporate network.

  The issue of session persistence raises the distinction between communication breakdown and a lack of communication where the latter refers to a VPN work session purposely left open with no packets transferred (case of a fire truck terminal remaining online with firefighters out on the scene). In this instance, Mult-IP Gateways will maintain a live but otherwise idle session by issuing heartbeats at set intervals and expect client response.

- **Application persistence**

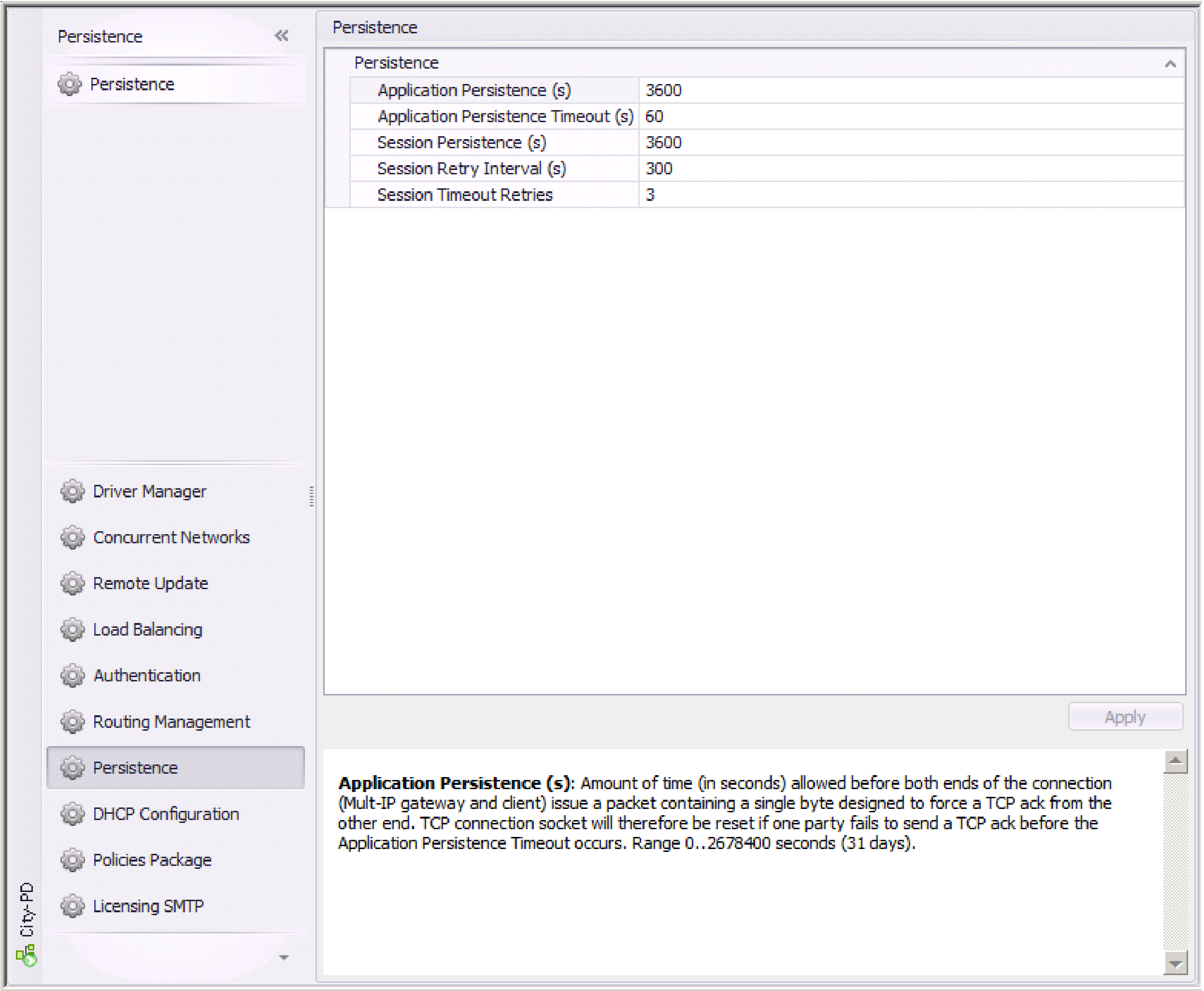
  Although Mult-IP has a built-in mechanism to support connection persistence over UDP, application persistence gives you additional control over TCP-mode connections. Its purpose is to issue a TCP connection reset if no activity is reported on the open socket beyond a preset amount of time. This mechanism may be useful in cases when an application server's TCP stream intended for a given client is interrupted due to any kind of network failure, while the concerned application lacks the ability to verify active connections.

  Another use for application persistence would be to force all pipe connections to close if the mobile client is out of coverage for an extended period. In practice, an out of coverage situation would then prompt retries and if the number of unsuccessful retries extends to the out of range timeout, then the pipe would report as unusable, causing Mult-IP to close all connections for that pipe.

Note: In a load-balancing environment, any condition causing all communication drivers onboard a given mobile client to appear out of coverage, may prompt client to scan for an alternate gateway. If the client reconnects and registers to an alternate gateway, all sockets previously open would inevitably be reset.

To set connection persistence,

1. Log on to the management console with group administration privileges.
2. Expand the system tree and select the functional group whose connectivity persistence you wish to configure.
3. Click the **Persistence** tab from the group workspace and review parameter description.



Persistence

Application Persistence (s)	3600
Application Persistence Timeout (s)	60
Session Persistence (s)	3600
Session Retry Interval (s)	300
Session Timeout Retries	3

Application Persistence (s): Amount of time (in seconds) allowed before both ends of the connection (Mult-IP gateway and client) issue a packet containing a single byte designed to force a TCP ack from the other end. TCP connection socket will therefore be reset if one party fails to send a TCP ack before the Application Persistence Timeout occurs. Range 0..2678400 seconds (31 days).

Parameter Description

Parameter	Description
Application Persistence (s)	Amount of time (in seconds) allowed before both ends of the connection (Mult-IP Gateway and client) issue a packet containing a single byte designed to force a TCP ack from the other end. TCP connection socket will therefore be reset if one party fails to send a TCP ack before the **Application Persistence Timeout** occurs. Range 0..2678400 seconds (31 days).
Application Persistence Timeout (s)	Amount of time in excess of the **Application Persistence** timer allowed for acknowledgement before TCP connection socket is closed. Range 0..1800 seconds.
Session Persistence (s)	Countdown (in seconds) triggered by the first packet (on session open) received from client. If client experiences connection failure and recovers within the set timer interval,

	the first packet received by the gateway upon recovery will reset the session persistence timer without requiring registration. Note that timer is reset with each received packet. Range 0..2678400 seconds (31 days).
Session Retry Interval (s)	Amount of time in excess (in seconds) of the **Session Persistence** timer allowed before an additional ack packet is sent. Failure to reply within this “grace period” will trigger client registration. Range 0..1800 seconds.
Session Timeout Retries	Number of session check packet retries before session is considered dead. Clients reconnecting beyond this point will be forced to register.

DHCP Configuration

DHCP Relay

The Mult-IP gateway’s DHCP Relay Agent component is a Bootstrap Protocol (BOOTP) relay agent that relays Dynamic Host Configuration Protocol (DHCP) messages between Mult-IP clients and DHCP servers for different virtual IP networks.

The DHCP Relay Agent is compliant with RFC 1542, "Clarifications and Extensions for the Bootstrap Protocol." For each IP network segment that contains DHCP clients, either a DHCP server or a computer acting as a DHCP Relay Agent is required.

As such, it will allow Mult-IP to request IPs on specific virtual IP segments according to the policy group associated with the Mult-IP client.

Using Mult-IP Client Software

The Mult-IP client software is a small-footprint mobility VPN communications software which registers as a background service. Thanks to remote policy management, it requires no user intervention where all communication driver maintenance work is managed by the system administrator. Nonetheless, Mult-IP Client features two user-facing components.

First, the Network Dashboard graphical user interface complements the Mult-IP background service by displaying the IP address assigned on the virtual segment in addition to connection-related activities for troubleshooting purposes.

Second, an information deskband visible in the system tray provides instant visual notification of communication driver status using color-coded traffic-like indicators. In addition, right-clicking the deskband allows users to reset gateway connection after such events as network outages or as required by network administrators following major policy updates.

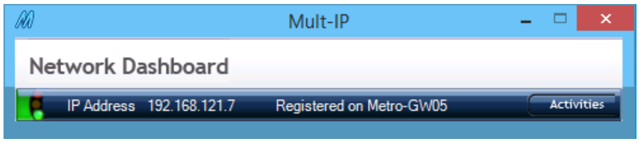
Note: Keep in mind that the Mult-IP Client software is an automatic service that starts with Windows. No User interface allows service stop/start.

Launching the Network Dashboard

The Network Dashboard automatically loads when a user's Windows session starts. Users may close the dashboard window or exit the GUI altogether by right clicking the system tray icon ( ) but this will not impact the background client service.

To start the Network Dashboard,

If for some reason the system tray icon and Network Dashboard are not showing, you may reload the application by clicking **Start** > **Programs** > **RadioIP** > **Mult-IP** > **Mult-IP Dashboard**. The following Network Dashboard will be displayed following a brief initialization period.



IP Address 192.168.121.7

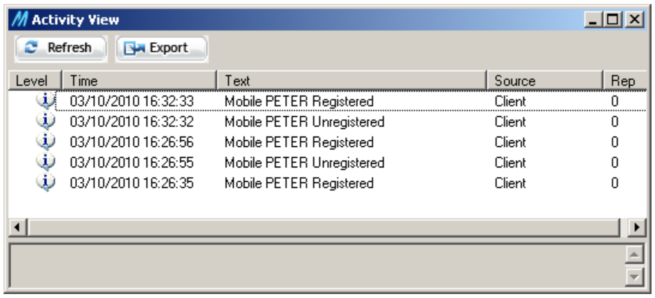
Registered on Metro-GW05

The Network Dashboard displays the IPV4 address allocated to the client on the Mult-IP virtual segment along with the current gateway on which this client is registered. For further information about the color code, refer to the Client Deskband section Client Status Reporting

Displaying the Activity view

The Activity view is a handy display tool that lets users scroll through events related to connection and communication in general. Events are updated at 5-second intervals and range from negotiation and authentication requests to loss of communication with the Mult-IP Gateway. Users should always refer to the exact event syntax when reporting problems to their helpdesk.

This tool is provided for troubleshooting purposes and contents are read-only. To display the Activity view, simply click the Activities button. The following will appear as a hover window.



Level	Time	Text	Source	Rep
i	03/10/2010 16:32:33	Mobile PETER Registered	Client	0
i	03/10/2010 16:32:32	Mobile PETER Unregistered	Client	0
i	03/10/2010 16:26:56	Mobile PETER Registered	Client	0
i	03/10/2010 16:26:55	Mobile PETER Unregistered	Client	0
i	03/10/2010 16:26:35	Mobile PETER Registered	Client	0

From there:

a) Click Refresh to prompt event update. This can be useful in severe and timely troubleshooting situations.

b) Click Export to save a log of the latest 50 events in a .CSV (coma-separated value) file which can then be forwarded and retrieved in a spreadsheet application for analysis.

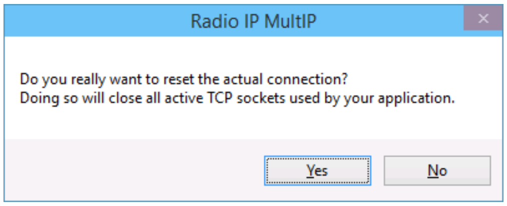
Resetting Client Connection

Resetting the active connection can be triggered remotely from the management console or performed locally by the field user for forcing mobile client reconnection to the gateway. A **Reset Connection** usually takes place when group policies are updated (prompted by a new authentication scheme or even an update to the client software), calling for immediate user attention.

Keep in mind that resetting a mobile client connection causes all open application sockets to be closed and potentially a DHCP address renew. However, DHCP reservations remain unaffected.

To reset a connection on the client side,

1. Right-click the Mult-IP Client system tray icon ( ) and select **Reset Connection.**



Do you really want to reset the actual connection?
Doing so will close all active TCP sockets used by your application.

2. Click **Yes**.

Restoring Factory Defaults

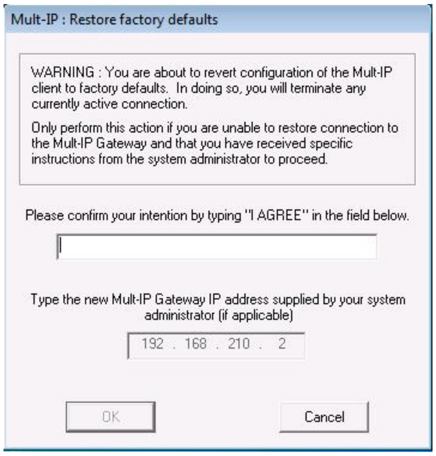
A handy restoration option is provided to help users recover from unhandled configuration settings caused by operator mistake or hardware exception. In effect, restoring to factory defaults resets Mult-IP Client to its newly installed state, with support limited to the Generic IP driver. This option should only be used as a last resort since it will erase all Mult-IP policies and reapply the entire set of policies that prevail at the time the mobile client is reassigned to its target functional group.

Note: To make use of this option and allow restored clients to reconnect with minimum resources, you are advised not to alter settings of the Generic IP driver supplied with the Mult-IP Gateway upon installation. You may however set an External Address Access for this communication driver to allow clients to reconnect from most field locations.

To restore to factory defaults,

Proceed as follows, if Mult-IP Client fails to respond despite extensive troubleshooting.

1. Try to secure a broadband connection to the mobile client via a wired or Wi-Fi connection.
2. Click the Mult-IP Client deskband area and select **Restore Factory Defaults** from the context menu. This will prompt the following dialogue.


Mult-IP : Restore factory defaults

WARNING : You are about to revert configuration of the Mult-IP client to factory defaults. In doing so, you will terminate any currently active connection.

Only perform this action if you are unable to restore connection to the Mult-IP Gateway and that you have received specific instructions from the system administrator to proceed.

Please confirm your intention by typing "I AGREE" in the field below.

Type the new Mult-IP Gateway IP address supplied by your system administrator (if applicable)

192 . 168 . 210 . 2

3. As requested, type “I agree” in the text area to unlock the IP address field. Notice that lowercase characters will be rendered uppercase by design.
4. Type the public IP address provided by the Mult-IP system administrator. This address is defined at the gateway level (in the External Address Access field of the Generic IP driver).

Note: Some organizations may prefer not to allow outside generic connections for security reasons. For instance, clients will need to be recalled and processed in-house if the **External Address Access** parameter is set to a local network (LAN) address. Otherwise, to make sure your mobile clients can connect in the field, type in a public address, then point to the mobile client’s functional group and successively apply **Reload Policies** and **Publish Policies**.

5. Click **OK** to initiate the restoration process. Allow several minutes for client to connect, authenticate, register and upload the latest default group policies.
6. Toggle **Protocol** to **TCP** or **UDP** to connect if the only communication driver available, namely the Generic IP driver, had its Connection Mode changed while client device is in the field. Manually setting protocol will allow client to connect and apply the latest policy change, which includes a connection mode change on some or all configured communication drivers.

Note: Unlike a **Reset Connection**, restoring factory defaults does not automatically assign clients to their functional groups. Similar to a new registration request, clients are quarantined upon reconnection, which requires operator acknowledgement.

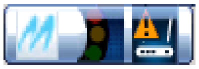
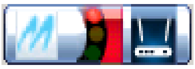
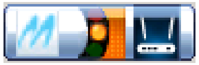
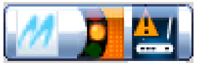
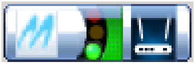
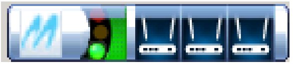
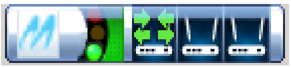
The Client Deskband

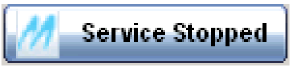
The deskband appears in the Windows taskbar. It uses iconic status indicators for a variety of Interoperable Radio IP products. Mult-IP uses the deskband to display connection status as well as the state of active communication drivers (in/out of coverage). This tool is a convenient alternative to the Network Dashboard, supporting real-time display of remote corporate network connection status without the need to rearrange the desktop or bring the Network Dashboard on top of other windows.

When hovering the deskband, a tooltip indicates the current registration status of the client and if registered, the gateway.

Client Status Reporting

The following table lists the statuses most commonly reported by the Mult-IP deskband.

Deskband status	Description
	**All indicators OFF** Client initializing. If this status persists more than a few seconds, look for software corruption. Please contact system administrator or vendor.
	**Red indicator** Client registered to gateway while quarantined pending operator acknowledgement. This status may also indicate a state of denied registration or authentication.
	**Orange indicator** Registration request sent upstream to Mult-IP Gateway. Flashing radio icon antennas indicate that client is either transmitting or receiving data.
	**Orange indicator** Client registered and authenticated but all communication drivers report as out of coverage.
	**Green indicator** Client registered to gateway and authenticated to functional group VPN session active.
	**Green indicator with multiple drivers** In this case, a policy was applied to all clients of a given functional group which contains a roaming profile made up of three drivers. Hover mouse over each radio icon to identify individual networks.
	**Green indicator with flashing radio icon** Indicates RX/TX activity on the active driver.

	**Mult-IP Client service offline** This exception may appear under abnormal CPU usage or in cases where antivirus programs quarantine (or prevent) applications at startup. To remedy this situation, restart the **Radio IP Mult-IP** service from the services console.

Reporting System Events

Mult-IP supports the following reporting tools:

Mult-IP Analytics: a robust tool designed to collect short to long-term data into detailed reports useful for system analysis, trending and auditing. Each report template provides detailed parameter snapshots over user set time intervals to help the decision making process in areas such as network infrastructure investments, mobile internet usage caps and so on.

Syslog: this tool sends CSV-type messages to a third-party SysLog collector. SysLog support addresses the needs of some users already using SysLog-based audit or data collection systems.

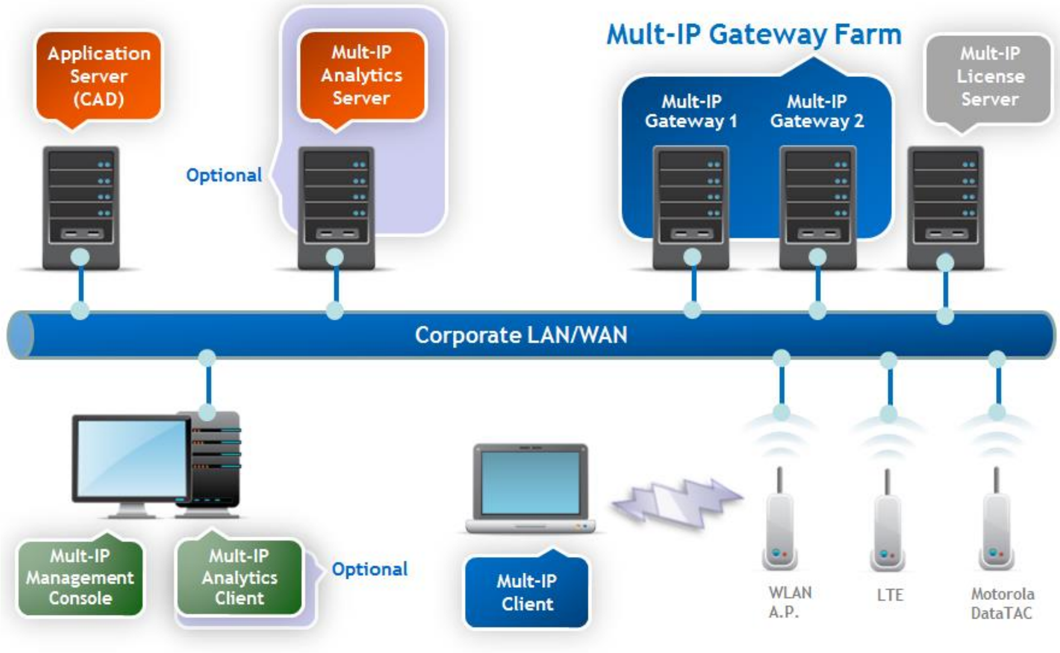
Note: Mult-IP outputs events to a single "systemlog" file at any given time, giving you the option of forwarding raw data to either Mult-IP Analytics or to a third-party SysLog server.

Mult-IP Analytics

The Mult-IP Analytics option comes with an extensive library of analytical report templates for the generation of informative and detailed reports on a wide range of system events, which include but are not limited to:

- **Application**: open sockets, version information
- **Network**: usage by application, fleet or individual clients; error count
- **Client-centric parameters over time**: authentication, registration, battery life, roaming patterns, compression usage, socket disconnects, OS details, quarantined
- **Gateway**: master/slave election count, load over time, top gateway usage

The following diagram identifies the constituents of the Mult-IP Analytics reporting chain.



To support this feature, a LAN-based physical or virtual Windows machine set to a static IP runs the SQL-based Mult-IP Analytics server software. System events originating from the master Mult-IP Gateway are fed to the SQL database at set intervals or as events occur.

The diagram shows the network-wide monitoring chain. Mobile clients are at the heart of the system and are susceptible to trigger the most events. Those add to gateway-generated events to supply the standalone SQL database with information that can be polled at any moment by management console administrators accessing the report template library.

Warning: the SQL database can grow rapidly for large fleet of several hundreds of user, make sure you have enough free disk and that you are not using the Express version of SQL in that case.

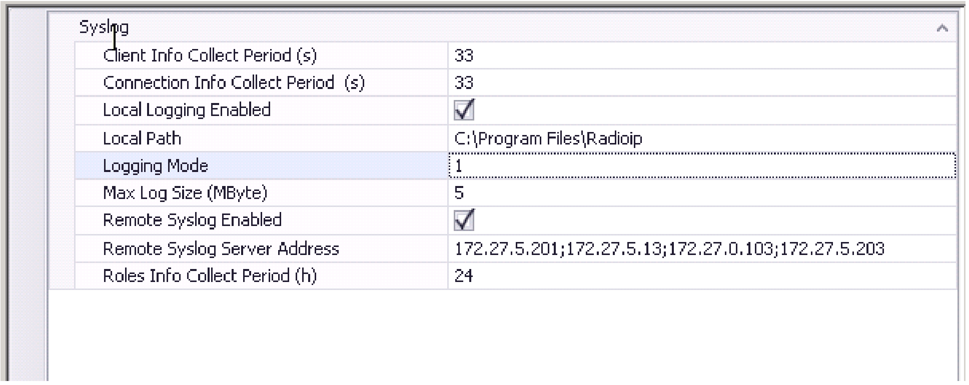
Report Configuration and Retrieval

This section describes the end-to-end process of configuring and retrieving reports. In short, you must:

- access features of the management console for the one-time task of setting system event forwarding to the Analytics reporting server;
- launch report queries through the Analytics launcher.

To configure system event forwarding,

1. Set aside a LAN-based machine to the task of reporting server and install Analytics server software. Take note of the static IP address assigned to this machine.
2. Log on to the management console with display/write access rights to the **Reporting** node.
3. Expand **Reporting** and select **SysLog** to set up reporting attributes.



Syslog

Client Info Collect Period (s)	33
Connection Info Collect Period (s)	33
Local Logging Enabled	☑
Local Path	C:\Program Files\Radioip
Logging Mode	1
Max Log Size (MByte)	5
Remote Syslog Enabled	☑
Remote Syslog Server Address	172.27.5.201;172.27.5.13;172.27.0.103;172.27.5.203
Roles Info Collect Period (h)	24

4. Check **Enabled** to allow parameter editing as per the next description table.

Table 10: SysLog Node Options

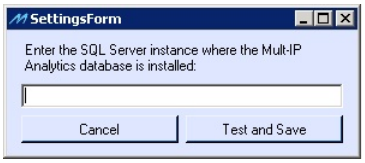
Parameter	Description
Client Info Collect Period (s)	Individual client status reporting frequency set to a default 3600 seconds.
Connection Info Collect Period (s)	Individual connection status reporting frequency set to a default 3600 seconds.
Local Logging Enabled	When checked, CSV log files are created and saved in the local path folder (see below).For heavy load system, this option may impact the general use of the gateway due to intense I/O on HD. When unchecked, CSV log files are not created.

Local Path	The default path in which log files are saved. Click the browse button to send files to a different location.
Logging Mode	Sets file generation interval. Type **0** for hourly, **1** for daily or **2** for weekly.
Max Log Size (MByte)	This setting determines the maximum CSV file folder size (in MB). Note that this setting closely relates to the desired file generation interval.
Remote Syslog Enabled	This parameter is used conjointly with the Remote Syslog Server Address. When checked, Syslog formatted messages are sent to each address of Remote Syslog Server Address. When unchecked: Syslog messages are not sent.
Remote Syslog Server Address	This parameter is used conjointly with Remote Syslog Enabled option. Enter the IP addresses of each of the Syslog Servers for which receiving Mult-IP Syslog messages is needed for reporting purposes. IP addresses are separated by ;.
Roles Info Collect Period (h)	This parameter updates the Analytics reporting server with the roles defined in the system at a set interval (expressed in hours). The reporting server uses this information to determine which user (according to his assigned role) is allowed to launch a given report query. By default, roles are updated every 24 hours.

5. Review your settings and click **Apply**.
6. Check **Enabled** again to enable event forwarding

To run Mult-IP Analytics reports,

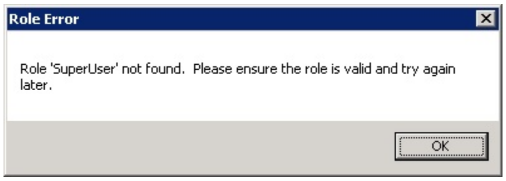
1. Log on to the management console with access rights to the **Reporting** node.
2. Click **Reporting** and select **Open Analytics Library** from the **Actions** pane. If you are accessing the reporting feature for the first time, you will need to supply SQL access credentials as shown next. Note that this dialog only appears once.



Enter the SQL Server instance where the Mult-IP Analytics database is installed:

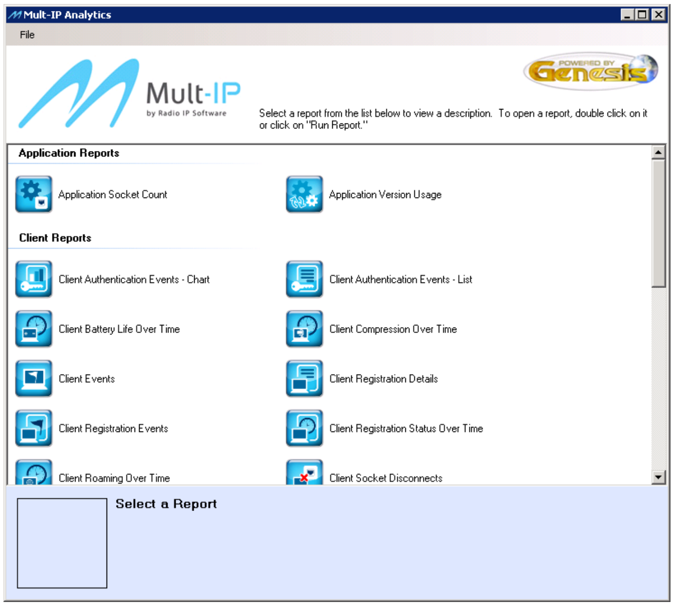
3. As stated, type in the SQL server instance specified during installation of the Analytics software.
4. Click **Test and Save** to continue with the list of report templates as shown next.

⚠ First time users may prompt the following after clicking **Test and Save**.



Role 'SuperUser' not found. Please ensure the role is valid and try again later.

This dialogue appears because the user accessing the reporting feature has been granted a new role that has not yet been updated in the Mult-IP Analytics server. This message will persist for up to 24 hour after role creation or for any custom amount of time set in the **Roles Info Collect Period (h)** field set in Reporting node, Syslog section.



Mult-IP Analytics

File

Select a report from the list below to view a description. To open a report, double click on it or click on "Run Report."

Application Reports

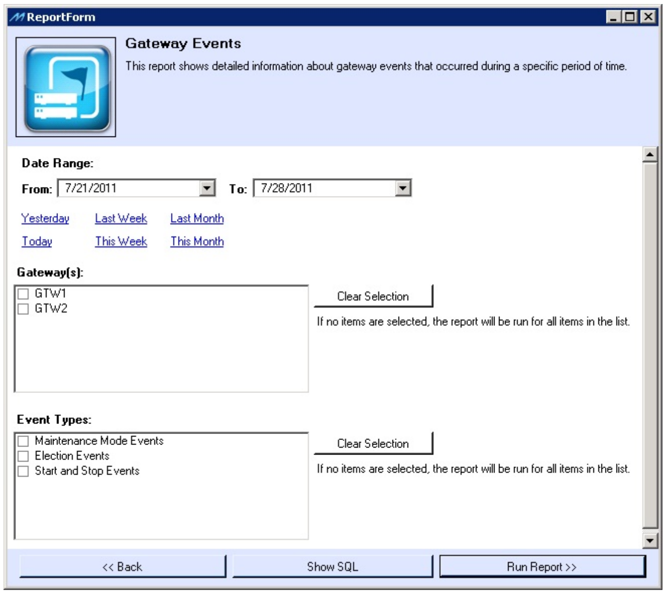
- Application Socket Count
- Application Version Usage

Client Reports

- Client Authentication Events - Chart
- Client Authentication Events - List
- Client Battery Life Over Time
- Client Compression Over Time
- Client Events
- Client Registration Details
- Client Registration Events
- Client Registration Status Over Time
- Client Roaming Over Time
- Client Socket Disconnects

Select a Report

5. Browse the report library and click the self-descriptive report title that matches the type of analytical data you wish to retrieve, then hit the **Run Report** hyperlink to view the report configuration form.



ReportForm

Gateway Events

This report shows detailed information about gateway events that occurred during a specific period of time.

Date Range:

From: 7/21/2011 To: 7/28/2011

Yesterday Last Week Last Month
Today This Week This Month

Gateway(s):

☐ GTW1
☐ GTW2

Clear Selection

If no items are selected, the report will be run for all items in the list.

Event Types:

☐ Maintenance Mode Events
☐ Election Events
☐ Start and Stop Events

Clear Selection

If no items are selected, the report will be run for all items in the list.

6. Use this form to specify search criteria:
   a) Enter the start and end date of the reporting period or click one of the preset ranges. Use extended reporting intervals for trend analysis.
   b) Set query filters specific to report context. Failure to set basic filter criterion will prevent report generation.
7. Click **Run Report** to launch query and display a comprehensive data report.

Report templates are non-protected Excel files. While you may save the displayed report as is, you should save reports under a new filename (using the **File** > **Save as** option in Excel) to keep your templates unaltered. Furthermore, remember that moving the report library files to a location other than that supplied after install will render the Analytics feature inoperable.

Syslog

The **SysLog** tool found under the **Reporting** node contains configurable parameters used to determine where SysLog messages (consisting of client activity, changing statuses and miscellaneous system-wide condition) are to be stored (in a local CSV file) or sent to an external machine that acts as a central SysLog server. Obviously, if you are connecting to a SysLog server while no link is available between the gateway machine and the SysLog server, the optional SysLog messages would then be lost. In such a case, SysLog messages stored locally on the gateway machine remain a viable source of troubleshooting information.

The SysLog protocol provides transport for devices targeted to send event notification messages across IP networks to event message collectors, also known as SysLog servers. The protocol is simply designed to transport event messages from the generating device, the Mult-IP Gateway, to the collector. Keep in mind that this UDP-type message means that the collector does not acknowledge log reception.

Various computer peripherals interfacing with the Mult-IP environment, from clients and gateways to routers, switches, Firewalls, VPN concentrators, and so on, are capable of generating SysLog messages for system information and alerts. For example, a Mult-IP Gateway might generate a SysLog message when a client IP goes silent or that some system configuration has changed. Similarly, a firewall can generate a SysLog message when it blocks a TCP connection.

Overview of the System Log File

To help you track log files in a queue, take note of the following filename convention. Notice that each file is date/time stamped:

RadioIPMultip_SystemLog_YYYY-MM-DD_HH-MM-SS.csv

The next list identifies Mult-IP events reported in the system log file as of this release.

Table 11: SysLog Report

Hex ID	MSG ID	TYPE	COMPONENT	TEXT	TRIGGER
7D0	2000	INFO	Connections	MSGID, Client Name, Client ID, Opening SYSTEM connection [Context: %1, Gateway source Name: %2, Gateway Source ID: %3]	When a client registers to a gateway.
7D1	2001	INFO	Connections	MSGID, Client Name, Client ID, Client IP, Application:%1, Version:%2, Network:%6, connection %5 opening to %3:%4 [Context: %7, Gateway source Name: %8, Gateway Source ID: %9]	When an application opens a socket
7D2	2002	WARNING	Connections	MSGID, Client Name, Client ID, Client IP, Application:%1, Version:%2, Network:%6, connection %5 failed to %3:%4 [Context: %7, Gateway source Name: %8, Gateway Source ID: %9]	When an application opens a socket and it fails
7D3	2003	INFO	Connections	MSGID, Client Name, Client ID, Client IP, Application:%1, Version:%2, Network:%6, connection %5 succeeded to %3:%4 [Context: %7, Gateway source Name: %8, Gateway Source ID: %9]	When an application opens a socket and it succeeds
7D4	2004	INFO	Connections	MSGID, Client Name, Client ID, Client IP , Application:%1, Version:%2, Network:%7, connection %5 closed to %3:%4, Duration:%6 [Context: %8, Gateway source Name: %9, Gateway Source ID: %10]	When an application closes a socket
7D5	2005	INFO	Connections	MSGID, Client Name, Client ID, Client IP, Application:%1, Version:%2, connection %3, Before Roaming Network:%4, Duration:%9, Tx Packets:%5, Rx Packets:%6, Tx Bytes:%7, Rx Bytes:%8, After Roaming Network:%10 [Context: %11, Gateway source Name: %12, Gateway Source ID: %13]	When an application roams between networks

Hex ID	MSG ID	TYPE	COMPONENT	TEXT	TRIGGER
7D6	2006	INFO	Connections	MSGID, Client Name, Client ID, Client IP, Application:%1, Version:%2, connection %3, Network:%4, Duration:%9, Tx Packets:%5, Rx Packets:%6, Tx Bytes:%7, Rx Bytes:%8, Compression: %10%% [Context: %11, Gateway source Name: %12, Gateway Source ID: %13]	Periodic message (configurable in seconds)
7D7	2007	INFO	Connections	MSGID, Client Name, Client ID, Client IP, Network:%1, connection %2 opening to %3:%4	When an application opens a UDP "socket"
7D8	2008		Connections	MSGID, Client Name, Client ID, Client IP, Connection %1, Network:%2, Duration:%7, Tx Packets:%3, Rx Packets:%4, Tx Bytes:%5, Rx Bytes:%6	Periodic message (configurable in seconds in the reporting node)
7D9	2009	INFO	Connections	Connection %1, Before Roaming Network:%2, Duration:%7, Tx Packets:%3, Rx Packets:%4, Tx Bytes:%5, Rx Bytes:%6, After Roaming Network:%8	When an application roams between networks
7DA	2010		Connections	MSGID, Client Name, Client ID, Client IP, Network:%1, connection %2 closed to %3:%4, Duration:%5	When an application closes a socket
BB8	3000		IPDriver	MSGID, Network name, Global Statistics, TX Packet:%1, TX Bytes:%2, RX Packets:%3, RX Bytes:%4, Broadcast Packets:%5, Broadcast Bytes:%6, Acks:%7, Naks:%8 [Context: %9, Gateway source Name: %10, Gateway Source ID: %11]	Top of every hour
BB9	3001		IPDriver	MSGID, Network name, Periodic Statistics, TX Packet:%1, TX Bytes:%2, RX Packets:%3, RX Bytes:%4, Broadcast Packets:%5, Broadcast Bytes:%6, Acks:%7, Naks:%8 [Context: %9, Gateway source Name: %10, Gateway Source ID: %11]	Periodic depending on configurable settings

Hex ID	MSG ID	TYPE	COMPONENT	TEXT	TRIGGER
3F0	1008		Gateway	MSGID, Client Name, Client ID, Client registration request, Network:%1 [Context: %2, Gateway source Name: %3, Gateway Source ID: %4]	When a registration message comes in
3F1	1009		Gateway	MSGID, Client Name, Client ID, Client IP, BatteryPower: %2, OS: %1, Group Name: %3, Group ID: %4, Client registration success [Context: %5, Gateway source Name: %6, Gateway Source ID: %7]	When a registration is accepted and NOT in a quarantine group
3F2	1010		Gateway	MSGID, Client Name, Client ID, Client registration rejected [Context: %1, Gateway source Name: %2, Gateway Source ID: %3]	When a registration request is rejected (whatever reason)
3F3	1011		Gateway	MSGID, Client Name, Client ID, Client IP, Client in Quarantine [Context: %1, Gateway source Name: %2, Gateway Source ID: %3]	When the registration is accepted into the QUARANTINE group
3F4	1012		Gateway	MSGID, ,CPU:%1%%, Memory:%2%%, Clients Connected:%3, Gateway load: %4 [Context: %5, Gateway source Name: %6, Gateway Source ID: %7]	Top of every hour
3F5	1013		Gateway	MSGID, ~~,~~ ,Gateway becomes master [Context: %1, Gateway source Name: %2, Gateway Source ID: %3]	When a status changes
3F6	1014		Gateway	MSGID, ~~,~~ Gateway becomes slave [Context: %1, Gateway source Name: %2, Gateway Source ID: %3]	When a status changes
3F7	1015	INFO	Gateway	MSGID, ~~,~~ Maintenance mode: Enabled [Context: %1, Gateway source Name: %2, Gateway Source ID: %3]	When a status changes

Hex ID	MSG ID	TYPE	COMPONENT	TEXT	TRIGGER
3F8	1016	INFO	Gateway	MSGID, ~~,~~ Maintenance mode: Disabled [Context: %1, Gateway source Name: %2, Gateway Source ID: %3]	When a status changes
3F9	1017	INFO	Gateway	MSGID, ~~,~~ Gateway starts [Context: %1, Gateway source Name: %2, Gateway Source ID: %3]	When a status changes
3FA	1018	INFO	Gateway	MSGID, ~~,~~ Gateway stops [Context: %1, Gateway source Name: %2, Gateway Source ID: %3]	When a status changes
3FB	1019	INFO	Gateway	MSGID, No more licenses available for mobile %1 in group %2 - Client will be moved in quarantine [Context: %3, Gateway source Name: %4, Gateway Source ID: %5]	When a client is refused registration because of licensing limitations
3FC	1020	WARNING	Gateway	MSGID, %1 [Context: %2, Gateway source Name: %3, Gateway Source ID: %4]	Text is either : ["Percentage of license used by clients reached %lu"], ["Number of gateways left %lu"], ["License will expire in %lu days"]
FA2	4002	INFO	Gateway	MSGID, Client Name, Client ID, Client IP, Client authentication request, User: %1 [Context: %2, Gateway source Name: %3, Gateway Source ID: %4]	When there is a client authentication
FA0	4000	INFO	Gateway	MSGID, Client Name, Client ID, Client IP, Client authentication success, User: %1 [Context: %2, Gateway source Name: %3, Gateway Source ID: %4]	When a client authentication is accepted
FA1	4001		Gateway	MSGID, Client Name, Client ID, Client IP, Client authentication failure, User: %1 [Context: %2, Gateway source Name: %3, Gateway Source ID: %4]	When a client authentication is rejected

Hex ID	MSG ID	TYPE	COMPONENT	TEXT	TRIGGER
1388			Clients	MSGID, Client Name, Client ID, IP address, Network:%1, Tx Packets:%2, Tx Bytes:%3, Rx Packets:%4, Rx Bytes:%5, Broadcast Packets:%6, Broadcast Bytes:%7, Acks:%8, Naks:%9, Compression: %10%% [Context: %11, Gateway source Name: %12, Gateway Source ID: %13]	Periodic message (configurable in seconds)
1389			Clients	MSGID, Client Name, Client ID, IP address, BatteryPower: %1 [Context: %2, Gateway source Name: %3, Gateway Source ID: %4]	When there is a change of 5% in battery power (lower of higher) from the last message (1009 or 5001)
138A			Clients	MSGID, Client Name, Client ID, IP address, Client back in coverage - Duration of out of coverage: %1 [Context: %2, Gateway source Name: %3, Gateway Source ID: %4]	When a client comes back in coverage
138F			Clients	MSGID, Client Name, Client ID, IP address, Lost Contact with client [Context: %1, Gateway source Name: %2, Gateway Source ID: %3]	When a session persistence expires.
1770			Group	MSGID, Group Name, Group ID, Group created [Context: %1, Gateway source Name: %2, Gateway Source ID: %3]	When a group is created
1771			Group	MSGID, Old Group Name: , Group ID, Group renamed to [%1] [Context: %2, Gateway source Name: %3, Gateway Source ID: %4]	When a group name is updated
1772			Group	MSGID, Group Name, Group ID, Group deleted [Context: %1, Gateway source Name: %2, Gateway Source ID: %3]	When a group is deleted
1B58			Role	MSGID, Role Name, List of Groups Names (IDs): %5, Gateway access: %6, Reporting access: %7, Role created [Context: %1, Gateway source Name: %2, Gateway Source ID: %3]	When a role is created

Hex ID	MSG ID	TYPE	COMPONENT	TEXT	TRIGGER
1B59			Role	MSGID, Role Name, List of Groups Names (IDs): %5, Gateway access: %6, Reporting access: %7, Role edited [Context: %1, Gateway source Name: %2, Gateway Source ID: %3]	When a role is edited
1B5A			Role	MSGID, Role Name, ~~,~~ Role deleted [Context: %1, Gateway source Name: %2, Gateway Source ID: %3]	When a role is deleted
1B5B			Role	MSGID, Role Name, List of Groups Names (IDs): %5, Gateway access: %6, Reporting access: %7 , Periodic information on Role [Context: %1, Gateway source Name: %2, Gateway Source ID: %3]	Periodic message (configurable in hours: from 1 hour to 1 week); Default: every 24 hours

Load-balancing Deployment and Maintenance

Mult-IP is a scalable VPN solution that allows you to add new gateways whenever factors such as fleet traffic increase to the point of affecting overall performance. Furthermore, the reliance on multiple load-balancing gateways provides redundancy in the event of planned or unplanned outages.

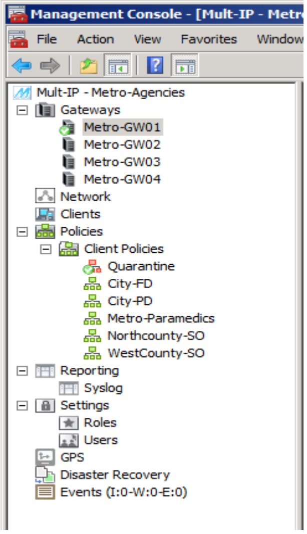
This section summarizes the steps required to deploy a load-balancing solution by aggregating knowledge acquired in both installation and administration guides. In an attempt to simplify the process, this section will assume that you have had a chance to test the software or at least, possess a good understanding of the system topology introduced on page 9.

As stated, the deployment process described below is valid for any type of installation. To facilitate the distinction, the specifics of load balancing are highlighted in **bold text**.

To deploy a Load-balancing Solution,

1. Review the Mult-IP Gateway installation prerequisites. **Notice that each load-balancing gateway host must be equipped with a Network Interface Card (NIC) dedicated to master/slave notification messages**.
2. “Ping” host names to validate connection.
3. Install Mult-IP Gateways. **While installing additional gateways, use the Scan Context utility to select the NIC assigned to host the Master IP address and to point each gateway to the context name broadcast by the first installed gateway**.

4. **Enable Gratuitous ARP announcements on all load-balancing gateways. The ARP packet informs LAN nodes of the new MAC address associated with the floating Master IP address. Remember to bind the discrete ARP packet <u>only</u> to the NIC dedicated to the Master IP address**.
5. Make sure that routes are in place to allow application servers to reach Mult-IP's virtual IP segment(s).
6. Install the management console on a workstation suitable for system administration. **Run the management console installer on all Mult-IP Gateways to supply resources needed for connections from x86 systems.**
7. Access the management console and acknowledge the presence of all your load-balancing Mult-IP Gateways under the **Gateways** node. Consider the following example where Gateway One is master as evidenced by a ( ) icon:
8.



- Mult-IP - Metro-Agencies
  - Gateways
    - Metro-GW01
    - Metro-GW02
    - Metro-GW03
    - Metro-GW04
  - Network
  - Clients
  - Policies
    - Client Policies
      - Quarantine
      - City-FD
      - City-PD
      - Metro-Paramedics
      - Northcounty-SO
      - WestCounty-SO
  - Reporting
    - Syslog
  - Settings
    - Roles
    - Users
  - GPS
  - Disaster Recovery
  - Events (I:0-W:0-E:0)

9. Perform basic system configuration **starting with the master gateway**:
   a) Configure gateway driver as described here.
   b) Run the **Configure Client Driver** wizard on each communication driver (except for the "0001 - Generic IP Driver"). Simply inspect each wizard screen making sure IP and port numbers match gateway specifications.
10. Click a slave gateway and notice that gateway drivers have been replicated. This time however, you must update IP and port so as to provide a unique combination for each driver:
    a) Type over the **External Address Access** and **External Port Access** to host specifics. In doing so, keep in mind that you may reuse an existing public address (if your address pool is limited) as long as the port value is different.
    b) Review the **Local Bind Address** for all drivers (disregard the "0001 - Generic IP Driver") and set each driver of each gateway to match the static IP of a dedicated NIC. Note that this step is optional but most IP environments recommend that individual communication drivers be bound to a single IP address. Keep the **Local Bind Port** value as it has been duplicated.
    c) Double-check driver settings for each gateway to ensure compliance to local firewall rules and run the **Configure Client Driver** wizard for each communication driver (except for the

"0001 - Generic IP Driver") for each slave gateway. Simply inspect each wizard screen making sure IP and port numbers match gateway specifications.

11. Create functional groups and set group policies for such features as pipe assignments, packet filter rules and authentication methods. Please review System Operation earlier in this guide for a complete overview of each policy feature.

Note: Avoid creating functional groups before step 10 is fully achieved. Moreover, avoid using the **Reload Policies** feature on functional groups created prior to this point, as you would run the risk of missing vital driver information.

12. Select a functional group and click the **LoadBalancing** tab in the workspace area.
13. Set **Registration Renewal Delay (ms)** to the amount of time (in milliseconds) allowed from the moment all communication drivers have reported a "gateway outage" condition to the moment clients are allowed to register to an alternate gateway on the basis of their originally assigned gateway still not reporting. A setting of 5000 (for 5 seconds) is recommended in most cases.

Note: The default **Registration Renewal Delay (ms)** value of "0" disables the feature.

14. Repeat the above for all functional groups and publish the new policies. The new settings will be pushed to mobile devices the next time they connect (or reconnect through **Reset Connection**).

Notice to operators of IP networks without Heart Beat : Please turn to Appendix E to learn about the Preferred Gateway feature used to supply the usable list of load-balancing gateways to mobile devices recovering from an out-of-coverage condition over HPD or IV&D networks.

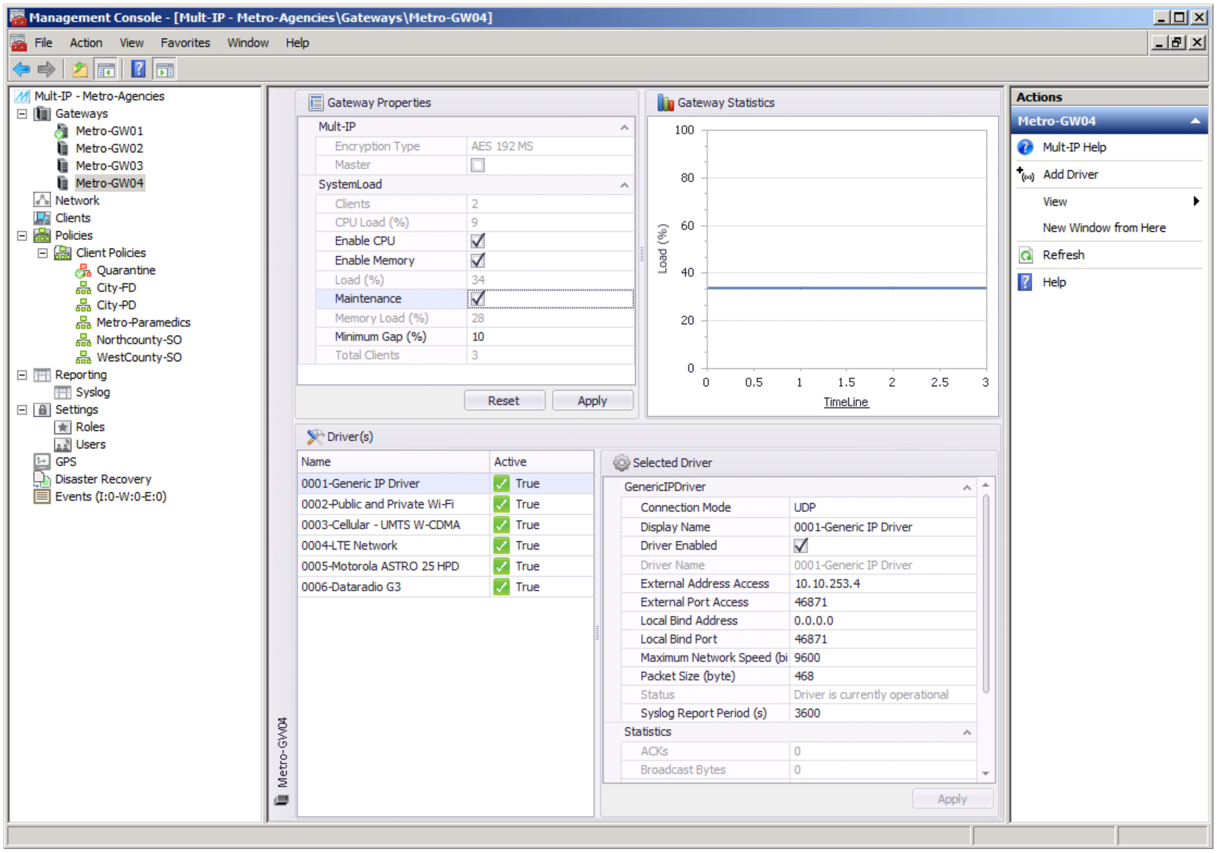
Planning system downtime using Maintenance Mode

Maintenance mode allows system operators to plan individual gateway downtime by redirecting mobile client to other load-balancing gateways on their next registration. This amounts to allowing traffic to trickle down to a point where the gateway can be safely shut down with no impact on fleet operation.

Note: New mobile clients, unaware of late gateway status due to a lack of policies, may register to a maintenance mode gateway. New clients are first quarantined, then assigned to a functional group at which point their connection is reset. Only when applying current policies upon reconnect will those mobile clients register to active load-balancing gateways.

To enable maintenance mode,

1. Select the gateway that you plan to take offline for maintenance purposes and point to the **Gateway Properties** pane.
2. As shown below, scroll down to **Maintenance** and check the box:



Gateway Properties

Mult-IP	
Encryption Type	AES 192 MS
Master	☐
SystemLoad	
Clients	2
CPU Load (%)	9
Enable CPU	☑
Enable Memory	☑
Load (%)	34
Maintenance	☑
Memory Load (%)	28
Minimum Gap (%)	10
Total Clients	3

Driver(s)

Name	Active
0001-Generic IP Driver	✓ True
0002-Public and Private Wi-Fi	✓ True
0003-Cellular - UMTS W-CDMA	✓ True
0004-LTE Network	✓ True
0005-Motorola ASTRO 25 HPD	✓ True
0006-Dataradio G3	✓ True

Selected Driver

GenericIPDriver	
Connection Mode	UDP
Display Name	0001-Generic IP Driver
Driver Enabled	☑
Driver Name	0001-Generic IP Driver
External Address Access	10.10.253.4
External Port Access	46871
Local Bind Address	0.0.0.0
Local Bind Port	46871
Maximum Network Speed (bi	9600
Packet Size (byte)	468
Status	Driver is currently operational
Syslog Report Period (s)	3600
Statistics	
ACKs	0
Broadcast Bytes	0

3. Click **Apply** to confirm. From this moment, traffic will slowly trickle to other load-balancing gateways as client connections are reset.

Note: Allow at least one minute for the maintenance mode request to propagate to all gateways.

Managing Product License

⚠	**Warning** If you deploy your Mult-IP license on a virtual machine, take the appropriate measures to ensure that your MAC addresses and machine identification cannot change over time. Failure to do so may result in a loss of license and potential outage.

License management calls for the enablement and maintenance of end-user software asset entitlement. Your Mult-IP license falls under one of two categories:

- **System-Wide License**: a license that accounts for the number of gateways, encryption type, maximum number of mobile devices, communication driver types and client platforms with no limitation to the number of definable functional groups. Upon registration, the system-wide Mult-IP license automatically applies to the Mult-IP organizational structure with limited user intervention.
- **Group-Level License**: a scoped license that characterizes the maximum number of simultaneous client connections as well as communication driver types applied to a single functional group. This licensing option is convenient for individual agencies assuming their own license fees, where each agency acts as a functional group in a larger organization. Group-level licenses require component association performed through the license console.

Note: Encryption type and gateway maintenance options apply to both license categories. They are considered global regardless of the number of functional groups added over time.

Registration-Free Trial Period

Your initial purchase entitles you to 30-days, registration-free operation which comes into effect on the date the first gateway is installed. It is imperative that you set your system up and supply Radio IP with registration information originating from the machine assigned as license server. Failure to meet this requirement within the 30-day trial period would render the product inoperable. Except for data encryption set to Single-DES, all features of the product are enabled during the trial period.

Note: An export Canada agreement is required to sell any software outside North America with a data encryption mechanism higher than Single DES.

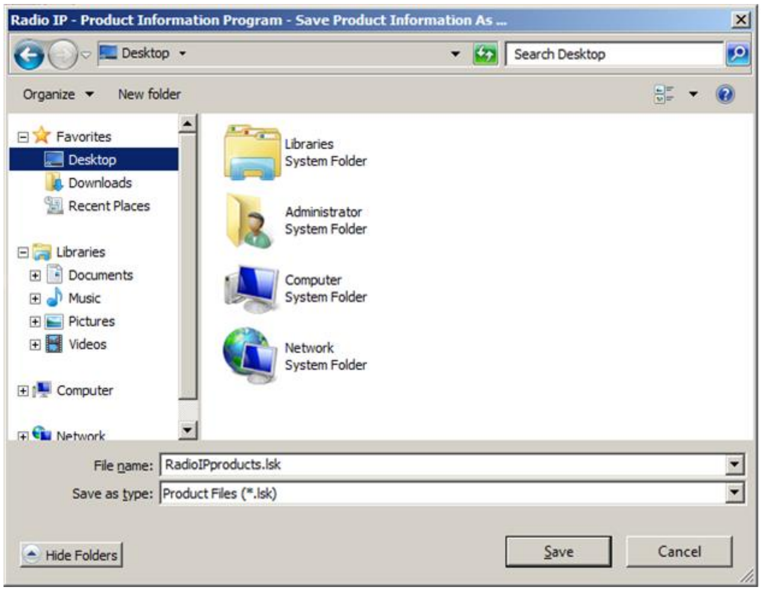
Registering Your Mult-IP License

Mult-IP registration is carried out on the machine assigned as license server within 30-days after installing the first Mult-IP Gateway. The next procedure shows you how to generate a product registration file to be sent to Radio IP for processing. In turn, Radio IP will issue the activation code specific to your product license type.

Note: All Mult-IP Gateways carry license management software. Therefore, any gateway can be assigned as license server for registration and asset monitoring purposes. However, you do have the option of hosting a license server on a standalone Windows 7 x64 or Windows 2008 R2 workstation to relieve gateway CPU usage. Review the *Mult-IP Installation Guide* for custom licensing server installation methods.

To register Mult-IP with an activation key,

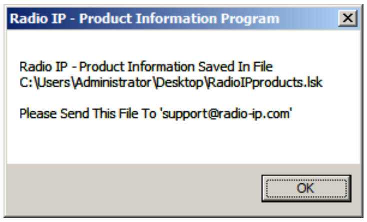
1. Log on to the machine assigned as license server.
2. Click **Start > All Programs > RadioIP > License Server** and click **Product Information**. This will open the product information generator utility.



File name: RadioIPproducts.lsk

Save as type: Product Files (*.lsk)

3. Click **Save in** to navigate to a known location on your hard drive, such as the desktop, where you want the *RadioIPproducts.lsk* file to be saved. **Important**: do not change filename.
4. Click **Save** to save the *RadioIPproducts.lsk* file.



Radio IP - Product Information Saved In File
C:\Users\Administrator\Desktop\RadioIPproducts.lsk

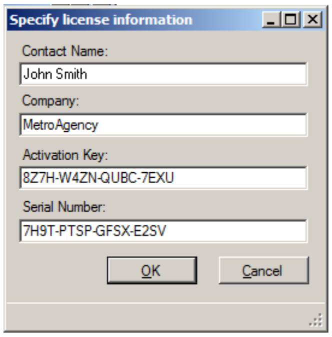
Please Send This File To 'support@radio-ip.com'

5. Take note of the file location and click **OK**.
6. Email the RadioIPproducts.lsk file to Radio IP at support@radio-ip.com for license processing. Radio IP will reply with a confirmation email containing information labeled as follows:

Contact Name	:	John Smith
Company	:	MetroCorp
Activation Key	:	XXXX-XXXX-XXXX-XXXX
Serial Number	:	XXXX-XXXX-XXXX-XXXX

7. Radio IP will issue a license file (*.lic) to be copied in the safe location on the master license server host.
8. Click **Start** > **All Programs** > **RadioIP** > **License Server** > **License Console** to launch a console dedicated to license rights management.

9. Click **File** > **Import License File** to view the following license information form.



Specify license information

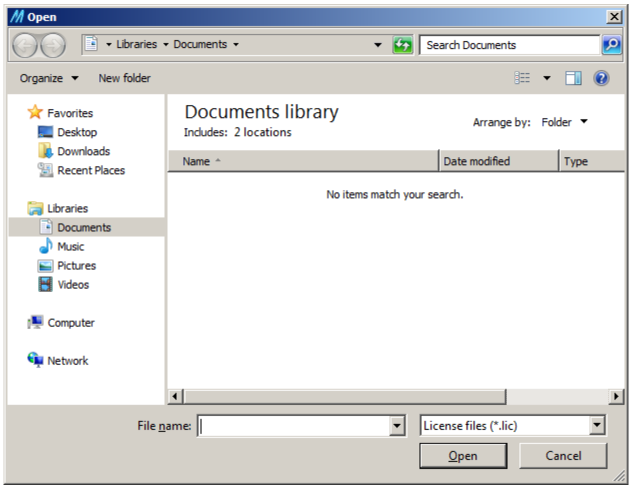
Contact Name: John Smith

Company: MetroAgency

Activation Key: 8Z7H-W4ZN-QUBC-7EXU

Serial Number: 7H9T-PTSP-GFSX-E2SV

10. Type customer information. You are encouraged to copy and paste **Activation Key** and **Serial Number** from the confirmation email to avoid typing errors. Keep a record of this information in a safe place.
11. Click **OK** to continue with the next dialog.



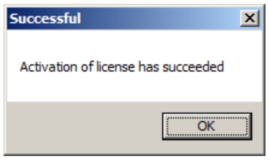
Open

No items match your search.

File name:

License files (*.lic)

12. Navigate to the safe location where the license file was saved, select *.lic and click **Open** to import license information into Mult-IP.



Successful

Activation of license has succeeded

Your Mult-IP product is now fully activated.

Once product activation is complete, the license server must remain online in order to perform real-time monitoring of registered assets. Should the license server machine fail or be powered down for any reason once it has been activated, you will have 30 days to put it back online or else, reapply the license activation process in order to assign the role of license server to a new machine.

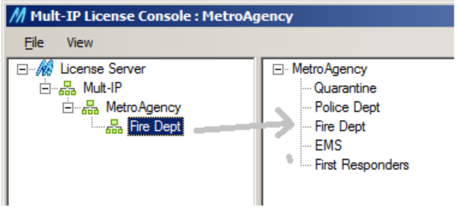
Applying group-level licenses

Additional steps are required when registering a group-level license designed to support an organization-scaled deployment over time.

To apply group-level license,

1. Complete the product registration process described in Registering Mult-IP.
2. Launch the license console and click **View** > **Group Association**.
3. Expand left-pane objects until you reach the license object identifier, which should closely match the naming convention of your defined function groups (right pane).

Note: The next screen sample illustrates a case where a group-level license is used to add the *Fire Dept* group to the system tree consisting in multiple agencies illustrated throughout this documentation. This serves to demonstrate how concurrent group-level licenses may be issued over time to suit the needs of a growing organization.

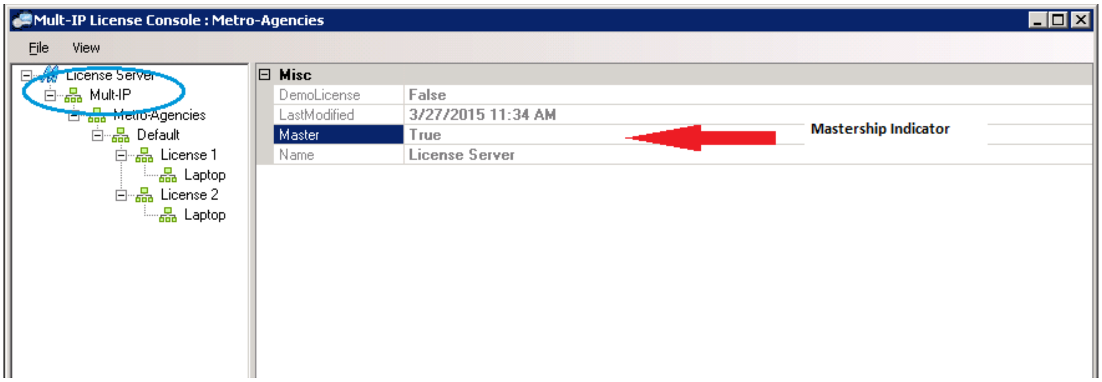


4. As shown, drag license object over corresponding unregistered organizational structure element.

No further action is needed. Simply close the license console. The license takes effect immediately as it propagates across all gateways (in a load-balancing environment).

License Console overview

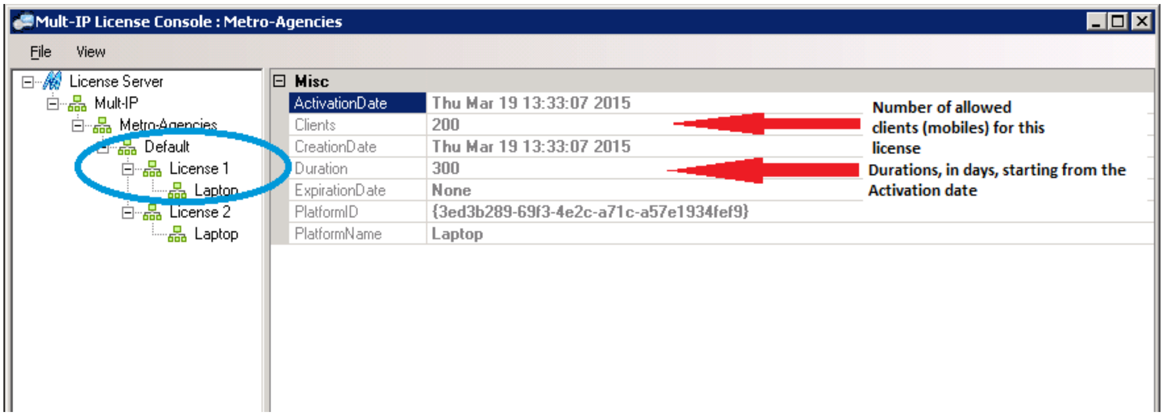
To find the gateway owning the License mastership, select the root item of the License Console.



DemoLicense	False
LastModified	3/27/2015 11:34 AM
Master	True
Name	License Server

Mastership Indicator

To find the number of allowed clients by the license or the duration of your license, navigate to the License level. Please take note that the licenses are cumulative. This means that you need to add up all the valid clients' counts (where the Expiration Date has not passed).

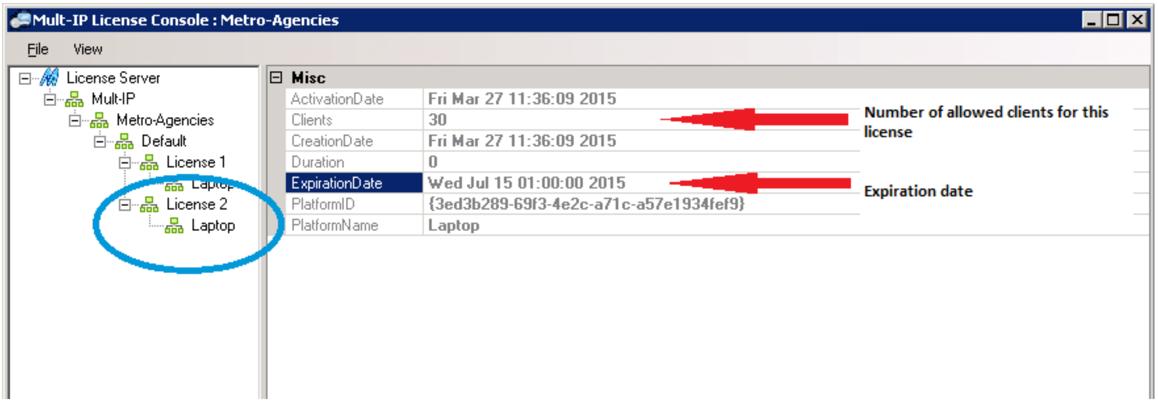


Misc	
ActivationDate	Thu Mar 19 13:33:07 2015
Clients	200
CreationDate	Thu Mar 19 13:33:07 2015
Duration	300
ExpirationDate	None
PlatformID	{3ed3b289-69f3-4e2c-a71c-a57e1934fef9}
PlatformName	Laptop

Number of allowed clients (mobiles) for this license

Durations, in days, starting from the Activation date

A registered license has no time restriction: Duration is set to 0 and Expiration date is set to "none". In the following example, the system allows 230 clients for the overlapped period and only 200 after.



Misc	
ActivationDate	Fri Mar 27 11:36:09 2015
Clients	30
CreationDate	Fri Mar 27 11:36:09 2015
Duration	0
ExpirationDate	Wed Jul 15 01:00:00 2015
PlatformID	{3ed3b289-69f3-4e2c-a71c-a57e1934fef9}
PlatformName	Laptop

Number of allowed clients for this license

Expiration date

License Lifecycle

Radio IP licenses offer great flexibility while extending only to those rights (such as the maximum number of mobile clients) you truly need. While customer licenses do not expire, others can be issued as partner leases or be awarded as part of pilot projects. In all cases, a built-in notification mechanism informs end-users ahead of reachable limits (or thresholds) such as:

- maximum number of mobile clients (75%, 90% and 100% of fleet size)
- number of load-balancing gateways (two, one, all allotments taken)
- advance notice on license expiration date:(3 months, 1 month, 7 days, 1 day, expiration date)
- maintenance contract end-date (1 year, 3 months, 1 week)
- communication failure between master gateway and license server

Note: Email notification of the master gateway machine's inability to communicate with the license server triggers a 30-day grace period which should prove long enough to resolve the situation.

Forwarding alarms

You may monitor license thresholds by reviewing license console status indicators, but do not see this as a requirement considering the frequency of built-in advanced warnings (see this list). Furthermore, Mult-IP offers the convenience of forwarding license-related alarms to email recipients.

Follow the next procedure to set up unattended license expiry alarm emails. This feature relies on SMTP (Simple mail Transfer Protocol) to alert administrative personnel in your organization.

To set up license expiry alarms to email recipients,

1. Launch the management console with sufficient access privileges.
2. In the context of a group license, select a functional group whose license expiry you wish to monitor or to be warned in case the maximum number of mobile clients allowed is reached.

Note: If you purchased a system-wide license, assign SMTP parameters to any one of your configured functional groups.

3. Click **Licensing SMTP** and set email parameters as per the following field descriptions.

Field name	Description
Email CC	Type the email addresses where alarms will be sent to in addition to the mail recipient(s). Addresses are separated by a semi-colon.
Email Destinations	Type the email address of main recipient. Use semi-colons to separate multiple entries.
Email Host	Type the machine name or IP address of the outgoing mail (SMTP) host.
Email Sender Address	Type the email address you wish to assign as alarm sender.
Email Sender Name	Type the email sender's display name as it will appear in the alarm message header.
Email Subject	Type a static subject line meant to attract recipient's attention.
Send Email	Enable to allow feature to generate emails on reached alarm thresholds.

4. Click **Apply** when complete.
5. Click the **Send Licensing Test Email** Action button to manually send a sample email. Use this handy feature to test SMTP configuration.
6. Select **Publish Policies** from Actions pane to save settings in the system configuration file.

Extracting and Configuring Traces

A tracing tool has been added to both gateway and client applications for extraction and configuration of traces which are messages stored in a file to keep track of steps taken by a program. The Tracing Tool is useful in troubleshooting/debugging situations.

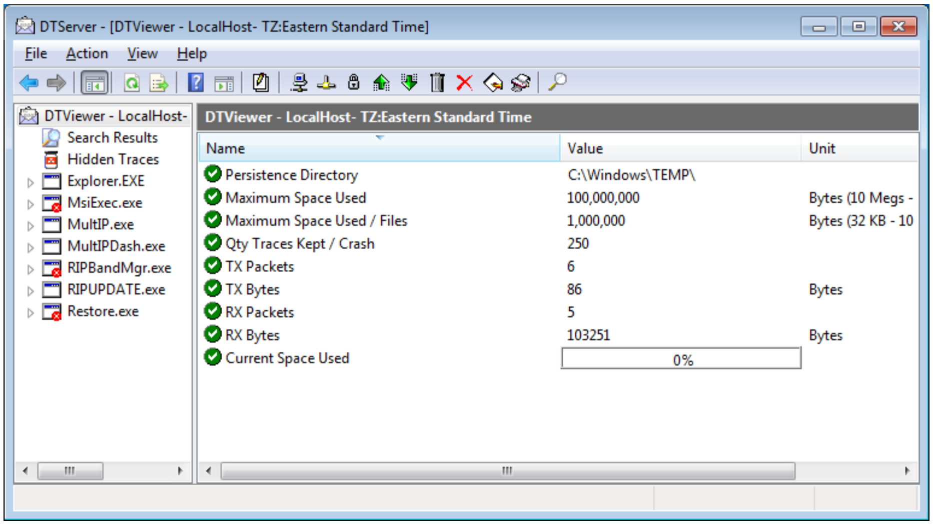
Sometimes, programs fail in hard to reproduce circumstances. For example, a connecting client may see its connection refused by the Mult-IP Gateway as soon as it is established. Surely because of some parameter mismatch, but it might be difficult to find which one. Traces are meant to address such problems. In a typical product-support scenario, Radio IP may very well recommend the System Administrator to turn on all tracing on the Mult-IP Gateway. Then the problematic client workstation would be asked to try connecting again with the assurance that hints, if not the solution to the problem, is logged in traces generated by the Tracing Tool. The System Administrator can then retrieve a trace file and forward it to Radio IP for analysis.

Warning: Turning on all traces is CPU-intensive and will adversely affect performance of both Mult-IP Gateway and client software. Tracing should therefore be limited to planned situations and should not be left running without purpose.

Mult-IP tracing is managed by an external program called DTViewer.

To open DTViewer,

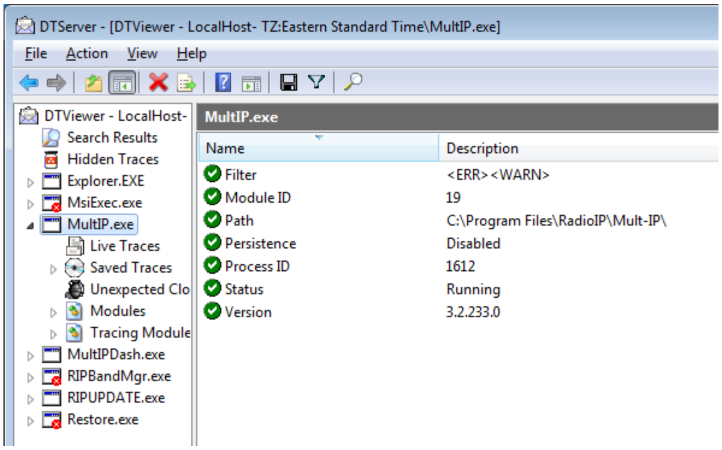
From either gateway or mobile client desktop, go to **Start** > **Programs** > **RadioIP** > **Diagnostic Tools** > **Tracing Tool**.



Name	Value	Unit
Persistence Directory	C:\Windows\TEMP\	
Maximum Space Used	100,000,000	Bytes (10 Megs -
Maximum Space Used / Files	1,000,000	Bytes (32 KB - 10
Qty Traces Kept / Crash	250	
TX Packets	6	
TX Bytes	86	Bytes
RX Packets	5	
RX Bytes	103251	Bytes
Current Space Used	0%	

The left pane lists trace client programs, i.e. capable of issuing traces. When collapsed, the list shows executables (.exe). Expand each item to reveal **Modules** and **Tracing Modules** subsets. The right pane lists properties of the selected program (or module).

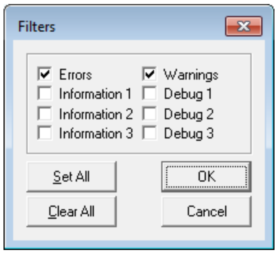
- **Modules:** This is the set of all modules used by the executable. Clicking a module reveals the following properties:
  - **Path**: File location directory.
  - **Status**: Running or Stopped depending on the state of the executable.
  - **Version**: Version string of the module.
- **Tracing Modules:** This is a subset of all components in the **Modules** list that have the special ability of generating traces. The following information is displayed in the right-hand pane upon tracing module selection (in addition to that provided by the Modules list).
  - **Filter**: File location directory.
  - **ModuleID**: A number identifying the module type (not the instance).
  - **Persistence**: Indicates the tracing status of the module (enabled or not).
- **DTViewer:** This is the tracing server. Its properties are special.
  - **Current Space Used**: Amount of memory currently used in the trace file.
  - **Persistence Directory**: Directory where traces are saved.
  - **Maximum Space Used**: Size of the circular trace file. Once the limit is reached, file writing deletes oldest traces.
  - **Maximum Space Used / Files:** Indicates the maximum size of each trace file saved.
  - **Qty Traces Kept / Crash**: Number of lines that are kept if Mult-IP fails.



Name	Description
Filter	<ERR><WARN>
Module ID	19
Path	C:\Program Files\RadioIP\Mult-IP\
Persistence	Disabled
Process ID	1612
Status	Running
Version	3.2.233.0

Filtering and Selecting Traces

To reduce the amount of information placed in the trace file, and to make tracing less CPU-intensive, tracing can be limited to a class of messages. To view the Filters window, simply right-click the top-level software item at the top level and select **Filters** from the context menu.



☑ Errors ☑ Warnings
☐ Information 1 ☐ Debug 1
☐ Information 2 ☐ Debug 2
☐ Information 3 ☐ Debug 3

- **Information traces**: notes about normal software behavior.
- **Debug traces**: notes of interest to the programmer/debugger.
- **Errors:** reports on abnormal conditions that could not be resolved.
- **Warnings:** reports on abnormal conditions for which the system took action. Warnings may also be reports of thresholds that are about to be reached, endangering the system.

To select the types of traces,

1. Select the EXE or tracing module whose traces you want to control.
2. Right-click and select **Filter** from the contextual menu.
3. Check boxes for the appropriate traces, click **Set** all to enable all trace types.

Enabling Trace (Persistence)

Note: To reduce the amount of information placed in the trace file, you are advised to purge memory of unnecessary data before continuing with this procedure. To do so, go to **Start** > **All Programs** > **RadioIP** > **Diagnostic Tools** > **Delete All Traces**.

To enable traces,

1. Select a trace client, such as MultIP.exe, from the left pane.
2. Lookup the **Persistence** module in the right-hand pane and notice its current status. If disabled, simply right-click and select **Enable/Disable Persistence** from the context menu to start traces.
3. Return to the DTViewer console after troubleshooting event has occurred to stop traces and create export file.

Appendix A - Common Configuration Notes

About Packet Size

The packet size parameter is present in the configurations of nearly all communication drivers. A few words ought to be mentioned about it.

The packet size setting is the maximum length of the data payload (including protocol overhead) to use on the Mult-IP communication network. The value results from a balance between efficiency and safety. The higher the number, the more efficient the communication becomes, as less overhead is used per data payload. However, the longer a packet is, the more susceptible it is to being corrupted by a transient RF emission, like radio interference, a starting engine, etc. Corruption leads to retransmissions, and efficiency is lost.

On many private networks, the maximum packet size is also determined by the network provider or by the modem manufacturer. Changing the values proposed by the driver installer should be made upon request by Radio IP or by your network provider.

About IP Routing

Both Mult-IP Gateway and Mult-IP Client installers supply their respective host computer with a virtual network interface card (VNIC). The VNIC has an IP address that is made available to the gateway so it may be used as a normal network interface in the Windows OS IP Routing Table. Since many options are given to the systems integrator by the client installer, this section will discuss the details of the IP routing table, and the various options offered to the user.

The IP Routing Table

An IP Route table is present in all computers with the IP stack installed. It allows the computer to determine where to forward an IP datagram when one is sent by a program. Here is what a routing table looks like. You can get this output on a Windows computer by typing “`route print`” from the command line.

```
Z:\>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 04 75 f5 82 e1 ...... 3Com EtherLink XL 10/100 PCI For Complete PC Man
agement NIC (3C905C-TX) - Packet Scheduler Miniport

===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface   Metric
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.95       20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      192.168.1.0    255.255.255.0     192.168.1.95    192.168.1.95       20
     192.168.1.95  255.255.255.255        127.0.0.1       127.0.0.1       20
    192.168.1.255  255.255.255.255     192.168.1.95    192.168.1.95       20
        224.0.0.0        240.0.0.0     192.168.1.95    192.168.1.95       20
  255.255.255.255  255.255.255.255     192.168.1.95    192.168.1.95       1
Default Gateway:       192.168.1.1
Persistent Routes:
None
```

What follows is a short description of the routing table structure and how it is used.

Network destination: This is a set of IP addresses or IP subnet that your computer can handle by itself. IP datagrams generated by the local computer are addressed. The target address is matched (up to some extent, as explained below) to one of these “Network Destinations”, and the best match made determines a line in the table, and the line determines a local interface (the interface column), and a gateway (the gateway column).

Netmask: This is a masking bit field. When comparing the target IP address in the datagram and the IP address in the network destination column, the comparison takes place inside the zone where the netmask bits are raised (set to 1). The more 1s you have in the netmask, the more determinative the match can be, and the better the match, the more precisely the routing can be determined. As a consequence, you can see in the table that no “Network Destination” is determined outside the bounds of the “Netmask”; it would be useless to do so. However, for a line to code the route it is intended for, the “Network Destination” must be determined entirely at least within the scope of the “Netmask”. As you can see in the above table, there is a line reading 0.0.0.0, which means that if no other line gives a match at all, at least this line will produce a 0-match. If a frame is sent to an address that matches no network destination in this table, then this line will be selected as giving a 0-match (poor, albeit a working default). The interface address on this line should be that of the **Default Gateway**.

Gateway: When a line is selected for routing, this field yields the IP address of the gateway (or router) where datagrams are forwarded for further routing.

Interface: This is an IP address bound to a local network interface card. When a line is selected for routing, this field determines the network card that should be used to send the frame. This structure allows a computer to host many network cards connected to entirely different networks.

Metric: The metric indicates the cost of using a route, which is typically the number of hops to the IP destination. Anything on the local subnet is one hop, and each router crossed after that is an additional hop. If there are multiple routes to the same destination with different metrics, the route with the lowest metric is selected.

Default Gateway: This line is considered the last resort routing solution, and will be associated to the default gateway, whose address you see at the bottom of the table, and a default interface. The default gateway (and the default interface) is where IP sends its traffic when the routing table does not provide any more appropriate information.

Appendix B - Port Assignment

This section identifies outgoing or listening ports that you need to open on corporate firewalls to permit communication between various components of the Mult-IP VPN.

Location	Port Value or Range	Description
Local gateway host firewall	19190 (UDP)	Default multicast communication port for Mult-IP systems
Local gateway host firewall	46871 (UDP)	Listening port reservation for the Generic IP driver. Used for client connection lifeline. Please do not change.
Local gateway host firewall	1024 to 65535 (TCP or UDP)	One listening port reservation for use by each additional communication driver.
Corporate firewall	46871 (UDP)	External port access reservation for the Generic IP driver. Used for client connection lifeline. Please do not change.
Corporate firewall	1024 to 65535 (TCP or UDP)	One external port access reservation for use by each additional communication driver.

Note: Mult-IP currently does not support firewalls on gateway hosts.

Note: Make sure to add Mult-IP processes to your Antivirus Exclusion list to prevent unexpected Mult-IP stops.

Appendix C - Predefined XML Entities

The XML language core to the Mult-IP solution configuration management and storage reserves five characters as predefined entities that must be avoided when editing text entry fields in the management console.

The table below lists the five XML predefined entities. The "Name" column mentions the entity's name. The "Character" column shows the character. To render the character, the format &name; is used; for example, &amp; renders as &. The "Unicode code point" column cites the character via standard UCS/Unicode "U+" notation, which shows the character's code point in hexadecimal. The decimal equivalent of the code point is then shown in parentheses. The "Description" column cites the character via its canonical UCS/Unicode name, in English.

Character	Name	Unicode code point (decimal)	Description
"	quot	U+0022 (34)	double quotation mark
&	amp	U+0026 (38)	ampersand
'	apos	U+0027 (39)	apostrophe *(= apostrophe-quote)*
<	lt	U+003C (60)	less-than sign
>	gt	U+003E (62)	greater-than sign

Appendix D - Integrating Motorola Public Service Broadband Networks

In its ongoing efforts to broaden industry support and keep pace with emerging technologies, Radio IP, in close partnership with Motorola Solutions, now supports the next-generation vehicular connectivity devices and mission critical handhelds by adding Motorola Solutions VSM communication drivers to the list of supported drivers. Implementation of the Motorola Solutions driver protocol offers benefits in multiple areas:

- mobile device traffic performance will be maximized due to the reliance on multiple simultaneous broadband radios;
- outbound and inbound requests (such as CAD transactions) will benefit from the low latency expected over OTA broadband
- Roaming handover occurs rapidly, further reducing occurrences of closing sockets due to prolonged out-of-coverage conditions. This aspect alone greatly enhances end-user experience.

Motorola Solutions LTE Vehicle Modems are designed for fast roaming between the following onboard wireless radios: Wi-Fi, EVDO, LTE provided by a Commercial Service Provider over LTE BC13 as well as the 700Mhz Public Safety LTE (LTE PSST BC 14).

To take advantage of Motorola Solutions LTE Vehicle Modem functionality, look for the following communication drivers in the Mult-IP IP driver family. They specify the interface for the Motorola Solutions VML700 LTE Vehicle Modem platform used on mobile data terminals (MDTs).

- Motorola WIFI
- Motorola EVDO
- Motorola LTE BC13
- Motorola LTE PSST

The Motorola Solutions VML700 LTE Vehicle Modem connects to the mobile device via cable or Wi-Fi (in which case the modem acts as a short range access point). Furthermore, each Motorola driver featured in this section provides underlying support for the Motorola Solutions UM1000 LTE USB modem plugged in the MDT as well as internal MDT Wi-Fi.

Always observe the following rules when activating the Motorola Solutions broadband family of Mult-IP drivers:

- **Motorola WIFI**: the MDT communicates over Wi-Fi used as a WAN either locally or through the Motorola Solutions VML700 LTE Vehicle Modem connected via cable.
- **Motorola EVDO**: the MDT communicates over the CDMA network available on the Motorola Solutions VML700 LTE Vehicle Modem connected to the MDT via cable or Wi-Fi.
- **Motorola LTE BC13**: the MDT communicates over LTE BC13 network available on the Motorola Solutions VML700 LTE Vehicle Modem connected to the MDT over cable or Wi-Fi.
- **Motorola LTE PSST**: the MDT communicates over the LTE PSST BC14 network available either on the Motorola Solutions UM1000 LTE USB modem plugged in the MDT or on the Motorola Solutions VML700 LTE Vehicle Modem connected to the MDT via cable or Wi-Fi.

Device integration extends to the Motorola Solutions LEX 700 Mission Critical Handheld enabling full management of handheld built-in interfaces (such as Wi-Fi, EVDO, LTE BC13 or LTE PSST BC 14) as well as VML700 LTE Vehicle Modem interfaces when connecting over Wi-Fi. To meet this goal, apply configuration to the four drivers featured in this section where each Mult-IP driver will be activated based on the following rules:

- **Motorola WIFI**: the LEX 700 Mission Critical Handheld communicates over its built-in Wi-Fi used as a WAN.
- **Motorola EVDO**: the LEX 700 Mission Critical Handheld communicates over an available CDMA network either through its internal interface or through the Motorola Solutions VML700 LTE Vehicle Modem via Wi-Fi.
- **Motorola LTE BC13**: the LEX 700 Mission Critical Handheld communicates over an available LTE BC13 network either through its internal interface or through the Motorola Solutions VML700 LTE Vehicle Modem via Wi-Fi.
- **Motorola LTE PSST**: the LEX 700 Mission Critical Handheld communicates over an available LTE PSST BC14 Network either through its internal interface or through the Motorola Solutions VML700 LTE Vehicle Modem connected via Wi-Fi.

For both scenarios identified in this section, adequate network selection is internally managed by way of Motorola Solutions software logic.

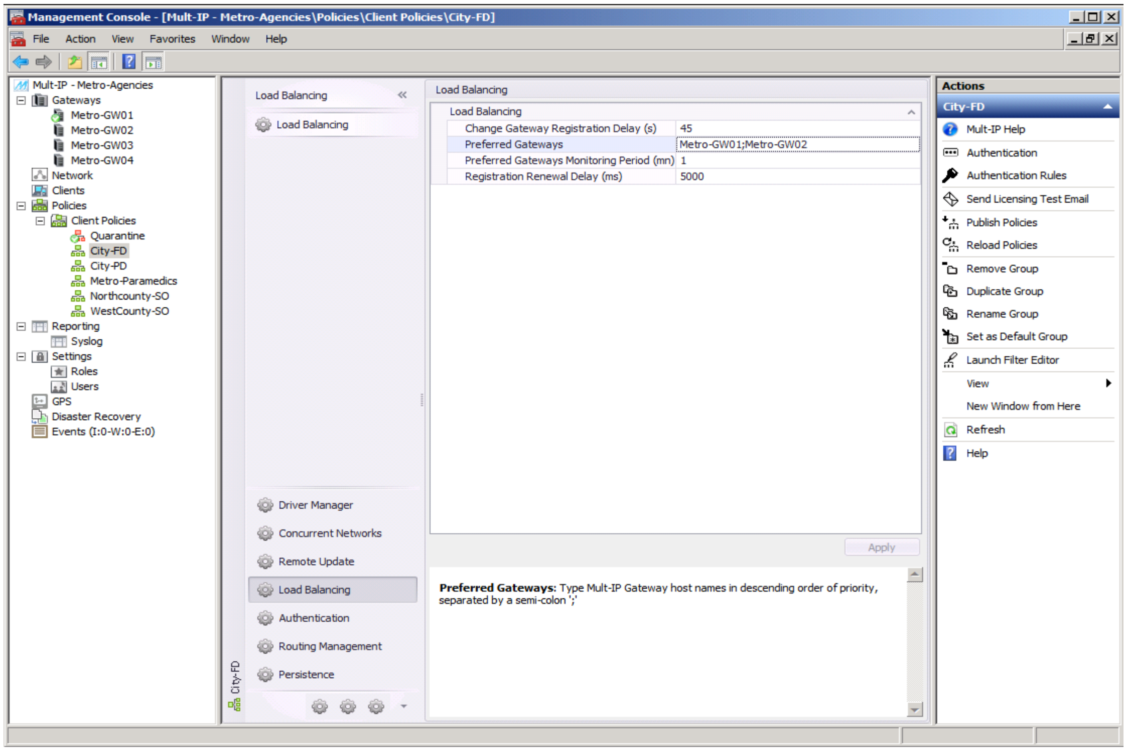
Appendix E - Preferred Gateways for IP drivers without Heart Beats

Preferred gateway is a load-balancing feature intended for operators of Motorola ASTRO 25 HPD, Motorola IV&D, CalAmp G3 and Harris' OpenSky networks. It assists mobile devices that cannot rely on heartbeats to track live gateways with a list of active gateways to look for when connecting. Once set, the list is pushed as a preferred gateway policy update that mobile clients of a given functional group apply whenever sending registration requests. This is helpful when a gateway goes offline during an out of coverage (OoC) conditions.

1. One by one, communication drivers report as "out of coverage" (OoC);
2. Once all communication drivers have reported OoC, Mult-IP Client enters discovery mode and scans the list of gateways for an opportunity to reconnect to the last-registered,
3. If reconnection fails due to an ongoing failure, registration attempt moves to the next Mult-IP Gateway down the preferred list.

To set the Preferred Gateway feature,

1. Select a functional group and click the **LoadBalancing** tab in the workspace area.
2. Click the **Preferred Gateways** field and type Mult-IP Gateway host names in descending order of priority, separated by a ";". The syntax should look similar to the following screen sample.



Management Console - [Mult-IP - Metro-Agencies\Policies\Client Policies\City-FD]

Load Balancing

Change Gateway Registration Delay (s)	45
Preferred Gateways	Metro-GW01;Metro-GW02
Preferred Gateways Monitoring Period (mn)	1
Registration Renewal Delay (ms)	5000

Preferred Gateways: Type Mult-IP Gateway host names in descending order of priority, separated by a semi-colon ';'

The **Preferred Gateways** feature requires that the following conditions be met in order to take effect.

- Make sure the Heartbeat Frequency setting is enabled for all communication drivers, except for Motorola ASTRO® 25 HPD and IV&D.
- Always identify at least two gateways in the list of preferred gateways published to clients.

The feature will be disabled if, during reporting, at least one non-IP driver reports as operational.

Table 12: LoadBalancing Tab Field Description

Field header	Description
LoadBalancing	
Change Gateway Registration Delay (s)	In a load balancing environment, duration (in seconds) after which a client will attempt to communicate with a new gateway when a reply to a registration request is not matched; Possible values are 10 to 120 seconds. Default value is 45 seconds.
Preferred Gateways	Type Mult-IP Gateway host names in descending order of priority, separated by a semi-colon "**;**"
Preferred Gateways Monitoring Period (mn)	Amount of time (in minutes) after a registration success before the client tries to register again. Default value is 0 (disabled), enable specifically for iVND, HPD and G3 drivers.
Registration Renewal Delay (ms)	Amount of time (in milliseconds) allowed from the moment all communication drivers have reported a "gateway outage" condition to the moment clients are allowed to register to an alternate gateway on the basis of their originally assigned gateway still not reporting. A setting of 5000 (for 5 seconds) is recommended in most cases. The default Registration Renewal Delay value of "0" disables the feature.

Glossary of Terms

API

An Application Programming Interface (API) is a specification intended to be used as an interface by software components to communicate with each other (an example of this would be to write an API for communication between a gateway and its database). An API may include specifications for routines, data structures, object classes, and variables.

ARP

Address Resolution Protocol. This protocol matches a host's IP address with the host's MAC address to ensure delivery of packets to the correct host.

Broadcast

The operation of sending network traffic from one network node, such as an application server, to all other network nodes, in this case, a fleet of mobile devices. A broadcast IP address forwards all messages that it receives to all addresses on the network.

Client Routing

The ability for a Mult-IP client to be used as a router device by other devices on the local Mult-IP client network, in order to get access to the Secured Network resources through the Mult-IP tunnel.

Concurrent Networking

Provides each mobile device of a given functional group the ability to run multiple simultaneous data streams over as many communication drivers. On the gateway side, a number of pipes are configured to handle specific application packets with each pipe assigned a subset of the available communication drivers in the same throughput performance range to maintain seamless user experience in out of coverage conditions. Concurrent networking means that video and other broadband applications travel over high-speed networks while mission critical narrowband packets are restricted to more resilient private radio networks.

Context

A discrete network signature defined during installation of the first Mult-IP Gateway. The context name is broadcast over the LAN and informs each subsequently installed gateway of the established virtual IP segment and master IP address. The context serves as a “hook” that binds all gateways working in conjunction.

Corporate Bypass

The ability for a mobile device to detect a network designated as secure based on preloaded policy information and stir traffic away from Mult-IP onto the designated network to mitigate gateway load. Corporate Bypass also implies that traffic is once again handled through Mult-IP as soon as mobile device leaves the designated location.

DHCP

Dynamic Host Configuration Protocol. DHCP is a protocol that allows network administrators to centrally manage and automate the process of assigning IP addresses.

DMZ

Demilitarized zone. Relates to an area of a corporate network connected to a firewall, which is accessible from both the Intranet and the Internet but has restricted access preventing public users from hacking into the Intranet. Typically, this is where public web/mail servers are placed in a corporate environment.

Encapsulation

The inclusion of a data structure (typically a packet) inside another packet for the purpose of hiding the first packet.

Ethernet

The most widely used local area network (LAN) technology; specified in the IEEE 802.3 standard.

Farm

A cluster of network server nodes. More specifically, a farm refers to a collection of at least two Mult-IP gateways operating in the same context for redundancy purposes.

Filter Rules

Filtering is a gateway mechanism that controls the data flow on the Mult-IP network. It refers to the definition and application of packet forwarding rules according to destination IP and port to a dedicated pipe. The general goal of such rules is to prioritize mission-critical packets by preventing unwanted traffic, susceptible to cause radio network slowdowns, especially over private mobile networks.

Firewall

A firewall can be either software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set.

Functional Group

A destination defined in the Mult-IP management console justified by organizational breakdown (into agencies) or by a common frame of reference between compatible mobile devices. Each group bundles an exclusive set of network performance, authentication, packet filtering and other miscellaneous parameters targeting a subset of an organization’s fleet devices through policies.

Gateway

A specific node within an organization Local Area Network that acts as an entrance to a separate network. The default gateway routes traffic to and from the separate network for delivery to the desired hosts at either end of the communication chain (mobile devices and application servers).

Gratuitous ARP (GARP)

An unrequested ARP message that is sent by a Mult-IP Gateway after a change has occurred so that all gateways in the same load-balancing farm can update their ARP tables with new information.

Guaranteed UDP

When employed over low latency broadband networks, UDP packets are qualified for guaranteed delivery by way of processing through Mult-IP's own Packet Manager, which oversees a packet checks not unlike TCP packets. Disabling this feature on a pipe experiencing heavy network traffic or using a narrowband network may lead to packet loss typical of the standard UDP protocol. Packet loss percentage is not software controllable since it is incumbent on network traffic.

GUI

Graphical User Interface. An interface, navigated with a mouse that has pictures and words on the screen with windows, icons, and pull down menus.

Hexadecimal

A base–16 number 0 – 9 or A – F representing 4 bits of a binary string; used for the Mobile IP key and the VPN key in user configuration files.

Hotspot

A location, such as an airport, hotel, or coffee shop, with broadband Internet access available to users for a fee. Typically, hotspots use Ethernet (wired) or wireless (WiFi) connectivity.

HTML

HyperText Markup Language. The language used to create World Wide Web pages with hyper-links and markup for text formatting.

HTTP

HyperText Transfer Protocol. The protocol most often used to transfer information from World Wide Web servers to browsers.

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is a widely used communications
Protocol for secure communication over a computer network, with especially wide deployment on
the Internet. Technically, it is not a protocol in itself; rather, it is the result of
simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

ICMP

The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is chiefly used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages. It is assigned protocol number 1.

Interface

A network adapter dedicated to a specific network radio or modem. Mult-IP Client-enabled devices are required to assign a unique name to each interface so as to bind individual adapters to their target communication driver.

IP

Internet Protocol. Part of the TCP/IP protocol suite, used to route packets from their source to their destination over the Internet.

IP address

A 32-bit binary number that identifies a specific host. The standard format for writing an IP address in IPv4 is dotted notation with 4, 8-bit octets.

ISP

Internet Service Provider.

LDAP

Lightweight Directory Access Protocol. An online service directory protocol. An LDAP directory contains entries which are a collection of attributes and a unique identifier.

Link

A connection between two peers over which data is transmitted.

Load-balancing

The sharing of fleet traffic between two or more gateways. This configuration in which one gateway, elected as master, manages the virtual IP network adapter at any one time, serves the purpose of reducing individual gateway load as well as providing redundancy in case of individual gateway failure.

Management Console

The MMC-based graphical user interface (GUI) used by Mult-IP administrators and other authorized personnel to perform configuration and monitoring duties. Depending on the installation location, the management console can be accessed from the desktop of any LAN-based workstation with visibility to the Mult-IP gateway context.

Master IP Address

Physical static IP address managed by the master Mult-IP Gateway used to route traffic from application servers to the Mult-IP virtual IP segment. The master IP address acts as a return path for packets sent back to mobile devices.

Metric value

The metric value associated with the network selected by the IP address of the router port. Permitted values are 0 to 16 with the default being 0. Selecting the default means that the network selected is a preferred (higher speed or shorter distance) route; while 1 through 16 specify routes of decreasing preference.

Mult-IP Client

The VPN software running on the mobile device that allows field users to access available corporate resources regardless of location.

Multicast

Communication between a single source host and multiple destination hosts on a network. (Standard Internet traffic typically requires a separate set of packets for each destination, multicast allows for one set of packets to be sent to multiple destinations.)

MVPN

Mobile Virtual Private Network. It provides mobile devices with access to network resources and software applications on their home network, when they connect via other wireless or wired networks.

NAPT

Network Address Port Translation. It is the process of modifying IP address information in IP packet headers while in transit across a traffic routing device.

NAS

Network Access Server. It is file-level computer data storage connected to a computer network providing data access to a heterogeneous group of clients.

NAT

Network Address Translation. An Internet standard that allows a network to use one set of IP addresses for internal traffic and another set of routable IP addresses for communication over the Internet. Certain protocols do not work through NATs by default and may require adaptation or tunneling to be applied.

Overhead

Refers to the time needed to send data packets over a given network, where each packet requires extra bytes of format information stored in the packet header. Overall transmission speed of the raw data is somewhat reduced by combining this information with the assembly and disassembly of packets.

Packet forwarding

The ability to pass IP packets on to another router (another network) for delivery to their final destination.

Pipes

A portion of the overall data stream between client and gateway dedicated to control traffic (in the case of the system pipe) or specific application traffic (pipes 0 thru 7) where multiple pipes can be use concurrently. Pipes are a component of the Mult-IP filter mechanism in which the administrator sets rules for the purpose of discriminating between packets according to the destination IP, port as well as transport mode (TCP or UDP).

Policies

Sets of configuration attributes designed to constrain the behavior of targeted mobile device within the boundaries of what it contains in terms of communication drivers, filter rules, authentication method and other miscellaneous connectivity parameters. Policies are defined at the group level and uploaded to gateway storage. They are then downloaded and applied by clients as they register to their target group.

QoS

Quality of Service (QoS) is the implementation of ranking policies aimed at improving bandwidth reservation and packet delivery for those applications deemed mission critical.

Quarantine mode

A locked down mode of operation for the Mult-IP Client that allows users to access only specific quarantined locations such as virus definition updates sites and patch update sites. Users are denied further access until the appropriate software checks and installations are completed.

RADIUS

Remote Authentication Dial-In User Service. RADIUS is the client/server, AAA protocol used for authentication and accounting.

Remote Update

As the name implies, the Remote Update feature allows system administrators to remotely update client software with minimum end-user intervention. Remote update is initiated at client registration, as soon as the system detects that a mobile device is running a version of Mult-IP Client earlier than the minimum set in functional group policies. This process is usually set to takes place over broadband networks only to preserve application bandwidth.

Roaming

The capability of a mobile device to access the Internet or corporate resources by seamlessly switching radio networks while maintaining an account for authentication and accounting with the same corporate entity.

Roaming Profile

Defines a sequence of network drivers into a policy used by clients to determine which driver to try in descending order of priority in the event of an out-of-coverage condition. A roaming profile is defined for each pipe and focuses on drivers best suited for the type of data routed to the pipe. For example, a pipe dedicated to video or file transfers will rely on a roaming scenario consisting only in broadband drivers.

Role

An assigned set of permissions that defines a user as having certain rights in the Management Console.

Source Code

A file created by a programmer that contains programming statements.

Split Tunneling

A networking feature that allows clients of a given functional group to bypass the Mult-IP Mobile VPN and access the connected local area networks while still relying on Mult-IP for mission-critical corporate applications and services, both of which are carried on the same physical connections.

SSID

Service Set ID. A character string that identifies a particular Wi-Fi access point.

TCP

Transmission Control Protocol. The TCP protocol establishes a connection between two hosts and guarantees the delivery of information between the hosts.

Traces

Timestamped accounts of individual Radio IP software events recorded using Diagnostic Tool and used for troubleshooting purposes.

Turnkey

An out-of-the-box installation method that accelerates deployment of the Mult-IP solution by bypassing such customization areas as communication drivers, functional groups, and so on. This method is valid for evaluation purposes.

UDP

User Datagram Protocol. This protocol provides a direct connection for hosts to send and receive packets over an IP network. UDP does not provide any error recovery and does not guarantee packet delivery.

Unicast

Communication between a single source host and a single destination host.

URI

Uniform Resource Identifier. FQDN followed by the port, protocol, and transport. (For example, AAA://aniara:2900;tcp).

URL

Uniform Resource Locator. The address of a file or resource on the Internet. The first part of the address defines which protocol should be used and the second part specifies the IP address or domain name where the resource can be found.

Virtual IP Segment

An IP address range completely isolated from that of the corporate LAN. The virtual IP segment, shared by gateways and mobile clients, is used for fleet mobile registration and internal routing. Scoped or non-scoped IP addresses and subnet masks may be supplied during installation of the first gateway and are applied by all gateways in the same farm.

VLAN

Virtual Local Area Network. A logical group of network devices that can communicate with each other as if they were physically located on the same LAN.

VPN

Virtual Private Network. A private data network that uses the public Internet to route data. The network secures its data and maintains its privacy through tunneling, authentication, and data encryption.

WiFi

Abbreviation for Wireless Fidelity used to identify wireless 802.11a/ac/b/g/n networks.

WINS

Windows Internet Naming Service. The service in Microsoft networks that translates hostnames to IP addresses.