

---

# ISAWS CONSORTIUM

## Coexistent Network Address Translation (NAT) Port Address Translation (PAT) Information Guide

August 2004

Version 0.0

---



# ISAWS Integration

## Network Address Translation (NAT) Port Address Translation (PAT)

---

### 1.0 Introduction to ISAWS NAT and PAT

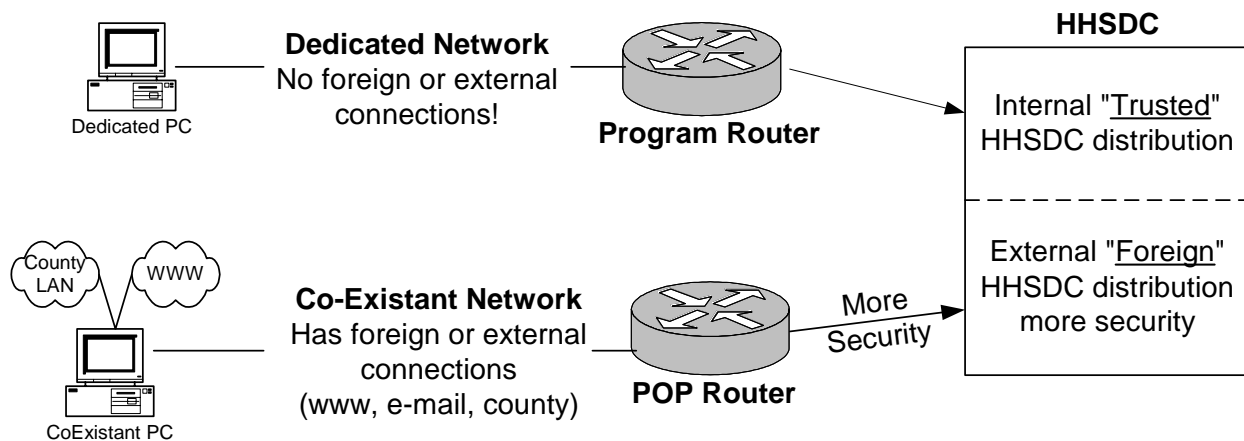
The objective of this paper is to provide historical information concerning the evolution of ISAWS network addressing. This document will include some configuration guidelines relating to county network connectivity to the Health and Human Services Data Center (HHSDC). Specifically, it discusses the introduction of Port Address Translation (PAT) as a complimentary feature to existing county networks currently using Static Network Address Translation (Static NAT).

Initially, County ISAWS connectivity to HHSDC consisted of workstations connected to hubs that were directly connected to an HHSDC router. Each workstation was assigned a static IP address that belonged to a subnet of registered IP addresses owned by HHSDC. These addresses generally fall into one of the three following HHSDC class B subnets, 158.96.x.x, 169.2.x.x or 169.3.x.x. These addresses were the only addresses that were allowed to travel onto the HHSDC network; all others were blocked. In many cases multiple routers and circuits were installed in a single location to service each individual program. This type of connectivity was referred to as dedicated connectivity. For ISAWS purposes this means that the only connectivity from the computer was to HHSDC. There were no other foreign connections to the county or to the Internet. As counties began to move towards a network that co-existed with other services, Network Address Translation and later Port Address Translation become important the county networking model.

### 1.1 Program Routers and Point of Presence Routers

As counties move from a dedicated network model to a coexistent model it is important to understand the different types of routers that HHSDC deploys. There are two primary types of routers that are deployed by HHSDC. If a county has a dedicated ISAWS network and has no foreign network connectivity, HHSDC will typically deploy what is known as a **Program Router**. If a county has a co-existent network or a network that connects to other foreign networks such as the Internet or a county LAN, HHSDC will typically deploy a **Point of Presence Router (POP)**.

### Program Routers vs POP Routers



Note that HHSDC has two primary points of entry. HHSDC has the trusted side for networks with NO outside connections and the Foreign side for networks with external connections. As soon as a county ISAWS network is connected to a foreign or outside network the county must utilize a POP router. The POP router has more security and is connected to the secure foreign distribution side at HHSDC.

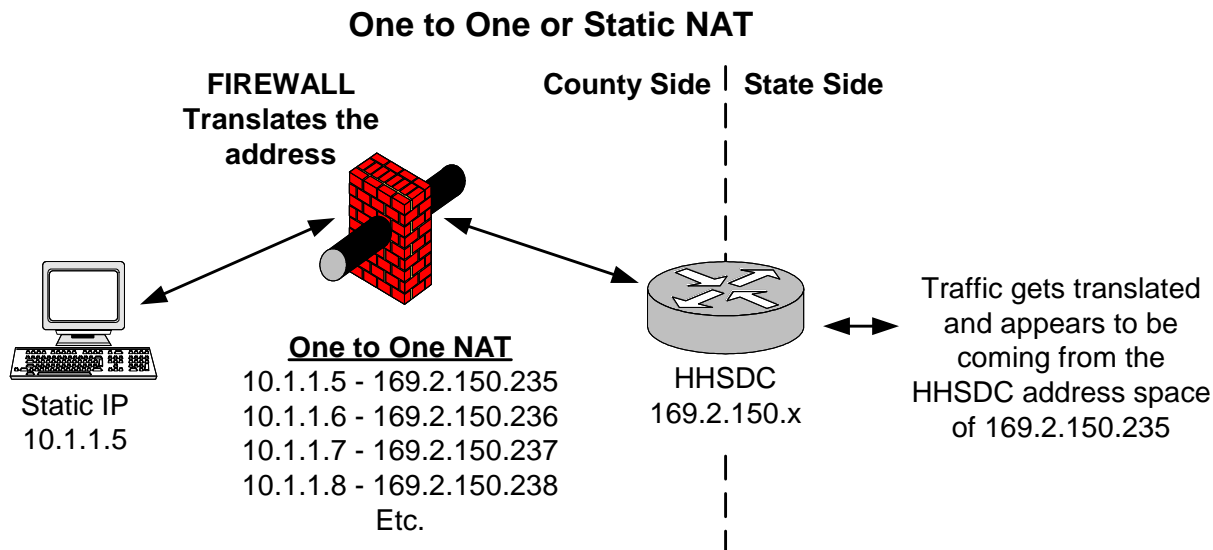
## 1.2 One POP per county

One of the most difficult parts about moving to a POP router is working within the HHSDC rule of only deploying one POP router per county. Each county is allowed only one POP router that all departments within the county must share. So all programs that connect to HHSDC and also connect to a foreign network, must share the same POP router within the county. This means that all departments within a county must work together and agree upon the location and administration of the POP router and the accompanying internal firewall and distribution devices. The department that is elected to support the POP router connection will be responsible for delivering services to all of the other departments that share that POP. It is recommended that county departments enter into Service Level Agreements (SLA's) in order to ensure that each department understands and agrees to the level of service that they will receive from the department supporting the POP.

## 2.0 NAT / PAT Functionality

Counties that would like to move to a co-existent network are required to obscure their private or registered addresses from HHSDC. HHSDC does not route private or registered addressing from foreign Third Party networks. Counties are advised to

renumber the local LAN and to utilize Network Address Translation (NAT) and possibly Port Address Translation (PAT) on the county firewall to obscure the renumbered county addresses from HHSDC. When traffic is routed to the HHSDC network it will be NAT'ed or PAT'ed to an HHSDC network address.

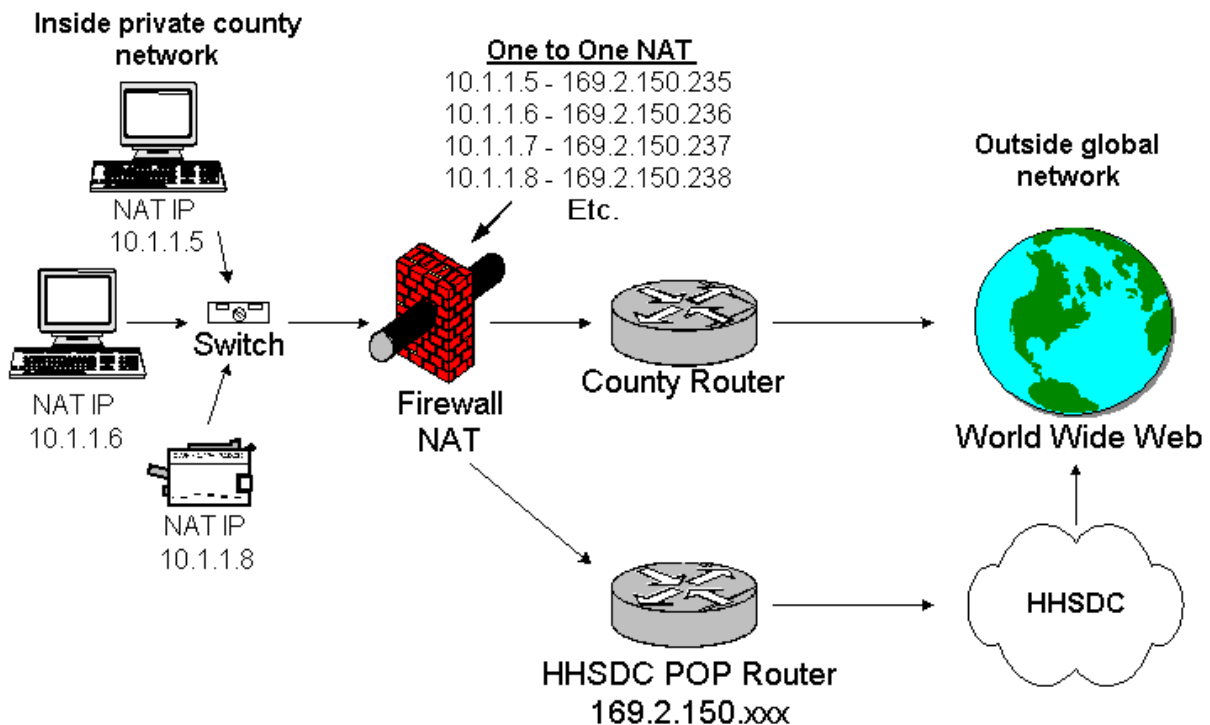


Note that the ISAWS workstation has been renumbered and currently has a static private IP address of 10.1.1.5. Renumbering to some other IP address is an HHSDC security requirement. HHSDC does not route county private IP addresses over their network. The address must then be translated to a state address before it enters the state network, in this case 169.2.150.238.

## 2.1 Configuring Network Address Translation (NAT)

Two key problems facing the Internet are depletion of IP address space and scaling in routing. Network Address Translation (NAT) is a feature that allows the IP network of an organization to appear from the outside to use different IP address space than what it is actually using. Thus, NAT allows an organization with private IP addresses to connect to the Internet by translating those addresses into globally routable public address. NAT also allows for an easier renumbering strategy for organizations that are changing Internet Services Providers or are voluntarily renumbering into classless interdomain routing (CIDR) blocks. CIDR and NAT are described in detail in RFC's 1519 and 1631 respectively at <http://www.ietf.org/rfc.html>

## One to One Static Nat with Internet



Note that each device in the county is addressed with a private static IP address. The address is mapped or translated **one for one** to a state IP address as the traffic is routed to the state network. HHSDC sees this traffic as coming from the HHSDC address space even though it originated from a private address of 10.1.1.x. Unfortunately there is a fair amount of labor involved in tracking each of the static private IP addresses in the county and understanding the state IP address that it corresponds to on the NAT device (firewall).

## 2.2 Practical Uses for NAT

NAT has several applications. First, NAT enables private IP networks that use non-registered IP addresses to connect to the Internet. NAT is configured on the router at the border of a stub domain (referred to as the *inside network*) and a public network such as the Internet (referred to as the *outside network*). NAT translates the internal local addresses to globally unique IP addresses before sending packets to the outside network.

As a solution to the connectivity problem, NAT is practical only when relatively few hosts on an inside network communicate outside of the domain at the same time. When this is the case, only a small subset of the IP addresses in the domain must be translated into

globally unique IP addresses when outside communication is necessary, and these addresses can be reused when no longer in use.

## 2.3 Benefits

A significant advantage of NAT is that it can be configured without requiring changes to hosts or routers other than those few routers on which NAT will be configured. As discussed previously, NAT may not be practical if large numbers of hosts in the stub domain communicate outside of the domain. (A stub domain is a domain, such as a county network, that only handles traffic originated or destined to hosts in that domain)

A router configured with NAT will have at least one interface to the inside and one to the outside. In a typical environment, NAT is configured at the exit router between a stub domain and backbone. When a packet is leaving the domain, NAT translates the locally significant source address into a globally unique address. When a packet is entering the domain, NAT translates the globally unique destination address into a local address. If more than one exit point exists, each NAT must have the same translation table. If the software cannot allocate an address because it has run out of addresses, it drops the packet and sends an Internet Control Message Protocol (ICMP) host unreachable packet. A router configured with NAT must not advertise the local networks to the outside. However, routing information that NAT receives from the outside can be advertised in the stub domain as usual.

## 2.4 More... NAT Terminology

As mentioned previously, the term *inside* refers to those networks that are owned by an organization and that must be translated. Inside this domain, hosts will have addresses in the one address space, while on the outside, they will appear to have addresses in another address space when NAT is configured. The first address space is referred to as the *local* address space and the second is referred to as the *global* address space.

Similarly, *outside* refers to those networks to which the stub network connects, and which are generally not under the control of the organization. Hosts in outside networks can be subject to translation also, and can thus have local and global addresses.

To summarize, NAT uses the following definitions:

**Inside local address** - The IP address that is assigned to a host on the inside network. The address is probably not a public IP address assigned by the Network Information Center (NIC).

**Inside global address** - A legitimate IP address (assigned by the NIC) that represents one or more inside local IP addresses to the outside world.

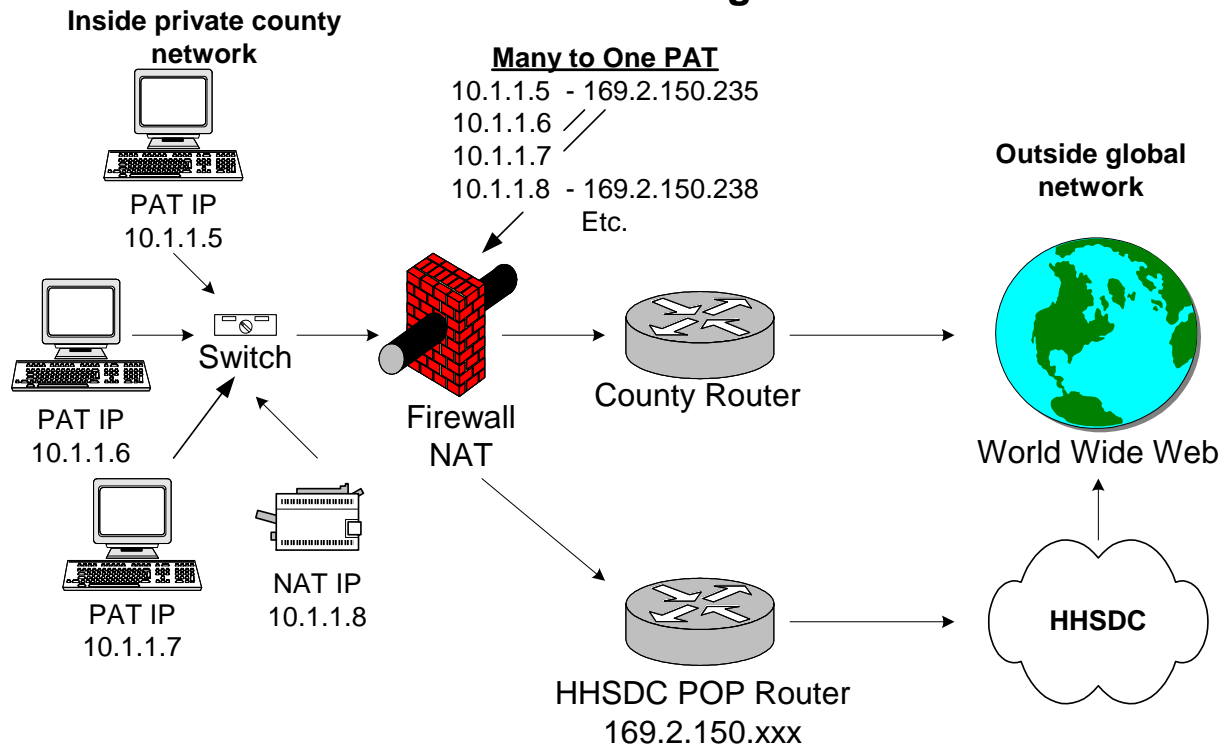
**Outside local address** - The IP address of an outside host as it appears to the inside network. Not necessarily a public address as it was allocated from address space routable on the inside.

**Outside global address** - The IP address assigned to a host on the outside network by the owner of the host. The address was allocated from globally routable address or network space.

## 2.5 Overloading NAT (PAT)

Conserving addresses in the inside global address pool can be facilitated by allowing the router to use one global address for many local addresses. When this overloading is configured, the router maintains enough information from higher-level protocols (for example, TCP or UDP port numbers) to translate the global address back to the correct local address. When multiple local addresses map to one global address, the TCP or UDP port numbers of each inside host distinguish between the local addresses. Port Address Translation extends existing NAT functionality from a “1 to 1” to a “many to 1” relationship of IP addresses. This is accomplished by associating the source port with each flow of the IP conversation. This many-to-one translation maps multiple IP addresses to 1 IP address. A unique source port number identifies each session, which conserves the number of registered IP addresses. The diagram below illustrates the many to one relationship from within the County network to HHSDC

## PAT Diagram



Notice how the inside addresses: 10.1.1.5, 10.1.1.6 and 10.1.1.7 are all translated to a single outside (state) IP address of 169.2.150.235. The printer 10.1.1.8 must use a one to one static NAT in our case it is 169.2.150.238.

### 3.0 PAT in the ISAWS Environment

The next stage in the development of the County/HHSDC network infrastructure took the form of router consolidation. The multiple-program-site's routing function was collapsed into a single router with multiple Ethernet ports, each port servicing a separate program. Separate and distinct IP subnets are assigned to each Ethernet port, and traffic was not permitted to flow from one Ethernet port directly to another. The bandwidth of the Wide Area Network (WAN) circuit to HHSDC is increased, and the number of circuits needed to service each site decreased from one for each program to one for each site.

A desire at the county level to access financial information, to utilize the Internet, and to implement common email systems lead to the development of county networks which began to connect county sites to each other. Most counties began acquiring personal computers and assigning them private IP addresses (10.x.x.x, 172.16. 20.x and 192.168.x.x). While these workstations could talk to each other, program workstations with HHSDC assigned IP addresses could not participate in the county networks due to

the incompatibility of the addressing schemes. A new network architecture needed to be developed that would allow program workstations and county workstations to communicate with each other and the Internet, while at the same time allowing only the program workstations to communicate with the mainframe applications located at HHSDC. NAT was introduced to allow this to happen.

With NAT, a county owned firewall or router was placed between the program workstations and the HHSDC router. The program hubs or switches were connected to the county hubs or switches and the program workstations were renumbered to the designated private subnet assigned to the site by the county IS department. Static routing table entries and integrated routing protocols (such as IGRP, EIGRP, RIP, OSPF, etc...) directed all traffic not destined for HHSDC to the core of the county network for disposition, and all traffic destined for HHSDC to the HHSDC router. Before leaving the county network, each program workstations IP address was statically translated into the registered address it had previously been assigned when it was a dedicated device on the former HHSDC subnet. This aggregation of county traffic could take place at each individual county site, or the county could install one Point of Presence (POP) circuit at a central location and translate all HHSDC traffic at the POP.

### **Routing Protocol Definitions**

IGRP – Interior Gateway Routing Protocol.

EIGRP – Enhanced IGRP.

RIP – Routing Information Protocol.

OSPF – Open Shortest Path First.

As time passed and more and more counties moved to the Co-Existent network architecture it became increasingly more difficult for HHSDC to maintain the static routing tables necessary to ensure that traffic flowed to, and only to, the specific county subnets from which it originated. Additionally, as the number of workstations increased, the scarcity of registered addresses owned by HHSDC became an issue.

As a result, PAT, which has historically been used for the translation of addresses for traffic destined for the Internet, and for several HHSDC applications such as MEDS and Integrated Statewide Information System, was re-examined. It became apparent that PAT could work for ISAWS and that it had several advantages when compared to Static NAT. Since numerous workstations could use a single IP address (plus a port number) instead of one unique address for each workstation, the total number of registered addresses required would be dramatically reduced.

While printers, ftp servers, and other hosts that need to be accessed by hosts at HHSDC will still need to have Static NAT entries configured in the POP firewall or router, all other workstations can utilize PAT for ISAWS connectivity.

The table below provides types of hardware and their corresponding configuration:

<b>Hardware Type</b>	<b>Configuration</b>
ISAWS PCs	PAT

Fiscal Workstations	NAT
Print Servers	NAT
DEPCON	NAT
EBT Embosser	NAT

## 4.0 Recommended Books

The following books contain information that may be helpful in completing county hybrid network projects.

### *The NAT Handbook: Implementing and Managing Network Address Translation*

**Author:** Bill Dutcher

**Publisher:** John Wiley & Sons; 1<sup>st</sup> edition (January 15, 2001)

**ISBN:** 0471390895

### *Cisco TCP/IP Routing Professional Reference*

**Author:** Chris Lewis

**Publisher:** McGraw Hill Text

**ASIN:** 0070410887

### *Cisco Switched Internetworks: VLANs, ATM & Voice/Data Integration*

**Author:** Chris Lewis

**Publisher:** McGraw Hill Osborne Media

**ASIN:** 0071346465

## 5.0 Information Resources and Credits

### Important Websites

Below are a list of information resources as related to this document.

Information on TCP\IP and RFC's obtained from <http://www.ietf.org/rfc.html>

Information on TCP\IP and Routing Definitions obtained from [www.cisco.com](http://www.cisco.com)

Helpful information on general networking <http://about.com/compute/>

## 6.0 Contact Information

### 6.1 ISAWS Consortium Office Contacts

Lauren Naughton	916-859-4968	<a href="mailto:lnaughton@isawsconsortium.org">lnaughton@isawsconsortium.org</a>	Technical
John Stinehelfer	916-859-4947	<a href="mailto:jstinehelfer@isawsconsortium.org">jstinehelfer@isawsconsortium.org</a>	Technical
Jeannie Pratt	916-859-4966	<a href="mailto:jpratt@isawsconsortium.org">jpratt@isawsconsortium.org</a>	Help Desk

### 6.2 Maintenance Center Contacts

Jerry Apsley	916-255-0465	<a href="mailto:japsley@isaws.cahwnet.gov">japsley@isaws.cahwnet.gov</a>	Mainframe
Ed Ayo	916-255-0404	<a href="mailto:eayo@isaws.cahwnet.gov">eayo@isaws.cahwnet.gov</a>	Tech Support
Jim Deeter	916-255-0433	<a href="mailto:jdeeter@isaws.cahwnet.gov">jdeeter@isaws.cahwnet.gov</a>	Tech Support
Greg Soria	916-255-0443	<a href="mailto:gsoria@isaws.cahwnet.gov">gsoria@isaws.cahwnet.gov</a>	WTW Support
Mark Eubanks	916-255-0447	<a href="mailto:meubanks@isaws.cahwnet.gov">meubanks@isaws.cahwnet.gov</a>	WTW Support
Chris Morrison	916-255-0519	<a href="mailto:cmorrison@isaws.cahwnet.gov">cmorrison@isaws.cahwnet.gov</a>	WTW Support
Thomas Scott	916-255-0488	<a href="mailto:tscott@isaws.cahwnet.gov">tscott@isaws.cahwnet.gov</a>	New Services
New Services	916-255-0488	<a href="mailto:newservices@isaws.cahwnet.gov">newservices@isaws.cahwnet.gov</a>	New Services
Production Control	916-255-0590		Production

### 6.3 HHSDC Contacts

Cindy Perkins	916-454-8087	<a href="mailto:cperkins@hhsdc.ca.gov">cperkins@hhsdc.ca.gov</a>	Customer Support
Steve Williams	916-454-7222	<a href="mailto:swillia6@hhsdc.ca.gov">swillia6@hhsdc.ca.gov</a>	Customer Support
Michael Shallcross	916-739-7742	<a href="mailto:mshallcr@hhsdc.ca.gov">mshallcr@hhsdc.ca.gov</a>	Network Engineering
Marc Hansen	916-434-7223	<a href="mailto:mhansen@hhsdc.ca.gov">mhansen@hhsdc.ca.gov</a>	Network Engineering
Daoud Antar	916-454-7231	<a href="mailto:dantar@hhsdc.ca.gov">dantar@hhsdc.ca.gov</a>	Network Engineering
Dave Winters	916-739-7633	<a href="mailto:dwinters@hhsdc.ca.gov">dwinters@hhsdc.ca.gov</a>	Network Installs
Support	916-739-7640		After Hours Support

### Change Control Log

Version	Change	Editor	Date
0.0			