
ISAWS CONSORTIUM

Coexistent Network Issues Guide

August 2004

Version 0.0

Table of Contents

1.0	Introduction.....	3
2.0	Pre Integration Considerations	3
3.0	Requirements	4
3.1	TCP/IP Protocol	4
3.2	Central Connectivity.....	4
3.3	Resource Skill Sets.....	5
3.4	Network Address Translation Device	5
3.5	Requirements Summary	6
4.0	Challenges	6
4.1	Domain Name Service (DNS)	7
4.1.1	Prescribed DNS Solution - DNS Zone Proxy Server.....	7
4.2	IP Routing	8
4.3	Netfinity Client.....	9
4.4	Network Address Translation (NAT)	9
4.5	ISAWS Supported Email.....	9
4.6	Timed Out Connections (EU Screen Recovery).....	10
5.0	DEPCON and Finance Workstations.....	11

ISAWS Integration – Coexistent Network Issues Guide

1.0 Introduction

Initial designs for a statewide welfare automation system were specific to welfare automation and did not address or accommodate other county automation needs such as email, groupware, Internet, internal host system access, and desktop management. To compensate, counties developed less than optimal solutions such as providing workers with multiple workstations. Counties quickly realized that the solutions available were inefficient and in many cases, ineffective.

To accommodate the changing automation needs of county business practices; counties identified a need to integrate county and ISAWS services onto a single workstation. This concept, commonly referred to as a hybrid network, entails “ISAWS Integration”.

A hybrid network consolidates the county data network with the data connection(s) from HHSDC. Through the implementation of a hybrid network, many counties today are able to provide access to systems such as ISAWS, MEDS, CMIPS, CMSNET, GEMS, WTW, county resources, and the Internet on a single workstation. This configuration allows ISAWS users to participate in the counties enterprise automation environment. Users are able to access all countywide and, or department wide shared resources and are presented with a seamless, “no barriers” environment.

Configuration, implementation, and maintenance of a hybrid network can pose challenges and may not be a viable solution for all counties. This document is intended to assist counties to evaluate the feasibility of implementing a hybrid network through the use of Network Address Translation (NAT). While counties can implement a hybrid network using other methods such as VLAN, this document focuses on NAT. For information regarding VLAN please contact Consortium staff to obtain VLAN supporting documentation.

Note: Counties unfamiliar with the features, limitations, and capabilities of the county network should contact the appropriate network equipment vendor(s). The appropriate vendor should also be contacted for specific steps to configure equipment.

2.0 Pre Integration Considerations

Counties considering an integrated ISAWS network should first evaluate the current automation environment. Considerations include but are not limited to the following:

- Does the county already have a wide area network?
- Are all offices connected with sufficient bandwidth data connections?
 - Are the connections T1?
 - Are the connections fiber?
 - Note: 56K connections may not be sufficient depending on the number of workstations to be supported, and whether the workstations will require access to the WTW application
- Does the county utilize and route the TCP/IP protocol (ISAWS Systems utilize the TCP/IP protocol)?
- Does the county have DNS and, or DHCP servers?
- Does the county have an existing email system or a group collaboration environment such as Exchange or GroupWise?
- Is the environment well managed and easy to manage?
- Is the County and or Social Services Information Technology staff capable of:
 - Providing the additional support required of the ISAWS machines?
 - Strategically planning an integration effort and testing the feasibility of such integration?
- Does the county have an existing shared broadband Internet connection?

Costs associated with the ISAWS integration effort are largely dependent on the existing infrastructure within the county. Counties may elect to have a feasibility study completed to determine the advantages presented to the end user, the associated costs, and develop a work breakdown structure necessary for an effective integration effort. Each county must evaluate the advantages and associated costs to make a final determination regarding ISAWS integration.

3.0 Requirements

Configuring a hybrid network environment requires consideration of key elements.

3.1 TCP/IP Protocol

The TCP/IP protocol defines how a network packet is transmitted and transported. In order to provide a shared connection to ISAWS services hosted at HHSDC the county network must be able to pass TCP/IP protocol based traffic to/from the desktop workstation to/from the HHSDC data center in Sacramento.

3.2 Central Connectivity

Each ISAWS County should have at least one Cisco router provided by HHSDC to connect the county or the county site to the HHSDC data center in Sacramento. Most counties have a data center or “computer room” that all remote county sites connect to.

Ideally all remote sites requiring access to ISAWS are connected to this county data center or “computer room”.

The county must have an HHSDC router installed at the central county data center. If there is not an existing router and communication circuit at the site, it must be installed to provide a central means of connectivity to HHSDC. If feasible, an existing connection may also be relocated to the central location. The central connection to HHSDC must also have a communication circuit with a speed of T1 (1.54mb/s) or greater to provide an acceptable level of performance when connecting a large number of ISAWS workstations. The central HHSDC connection can be transported over county circuits or fiber runs to the remote offices that require connectivity to ISAWS services.

3.3 Resource Skill Sets

Counties wishing to configure a hybrid network must have available resources with the appropriate skill sets, necessary to implement routing changes to the county wide area network (WAN) to properly transport the ISAWS TCP/IP packets.

3.4 Network Address Translation (NAT) Device

Another critical requirement for implementing a hybrid network is a router, firewall or other device capable of performing Network Address Translation (NAT). NAT allows a one to one translation of a given TCP/IP address set.

While many counties currently use a router or firewall to perform NAT, other devices can also support NAT. Some examples include:

- Open source operating system devices configured to perform NAT
 - Linux and FreeBSD using ipfw are examples of open source solutions that can accommodate robust (and free) NAT solutions.
- Counties using a specific brand of network devices and equipment may wish to inquire with that vendor if they offer a robust NAT solution.
- Windows based NAT solution
 - Utilities are currently available to provide NAT translation on a Windows based system, however performance considerations need to be reviewed.
 - In some situations, it may be appropriate for counties to elect to test a Windows based NAT solution.

Some large Counties may wish to implement a redundant routing solution consisting of at least two routing devices (routers or firewalls), capable of providing a truly “hot fail over” fault tolerance. A failure of the central device for even the shortest period of time will result in a countywide ISAWS connectivity failure. For redundant devices, it is critical that they provide a transparent failure tolerance solution.

In the event that a NAT device fails and the routed traffic is dropped, for any length of time, the ISAWS screens or EU’s can be left open on the mainframe. Users will be

unable to reconnect until each screen is reset¹ or the mainframe is rebooted. Resetting each screen can be a time consuming process and must be completed by ISAWS System Support.

3.4.1 Transparent Routing

Counties implementing a hybrid network must use a private TCP/IP addressing scheme. Private addressing consists of network addresses not routable via the public Internet. Private addresses must then be translated to an HHSDC recognized address to be routable on the HHSDC network. This translation, accomplished by NAT, allows the workstation to appear directly connected to the HHSDC network while the county network connection remains transparent to HHSDC.

Example Network Address Translation (NAT)

ISAWS workstation - private addressing IP address	192.168.1.155
HHSDC recognized address	158.96.xxx.xxx

Counties integrating ISAWS into a hybrid network environment should review the “HHSDC Foreign Network Connectivity Policy”².

3.5 Requirements Summary

- Must be able to transport/route TCP/IP traffic
- Must have central connectivity to all county offices needing ISAWS
- Must have a centrally located HHSDC router and T1 Comm. Circuit
- Must have network device that can provide NAT/PAT
- Must be transparent to HHSDC

4.0 Challenges

Configuring a hybrid network and integrating ISAWS into the county network is not without challenges. Some known areas in which counties typically experience issues are:

- DNS
- IP Routing
- Netfinity Client
- NAT
- Email
- Time Out (EU Screen Recovery)

The following is a detailed description of each challenge identified, and prescribed solutions.

¹ See “Time Out Connections (EU Screen Recovery)”

² Contact Consortium Technical staff to obtain a copy of the *HHSDC Foreign Network Connectivity Policy*

4.1 Domain Name Service (DNS)

Domain Name Service (DNS) is a name service that associates an easily read name with a corresponding TCP/IP address. Integrating the HHSDC network with a county network may result in challenges for seamless DNS.

Desktop configurations reference the DNS name record for a given TCP/IP address. This allows the desktop configuration to remain the same when a TCP/IP address is changed for an ISAWS resource. It also prevents connection outages when the TCP/IP address is changed.

When a workstation requests a connection to an ISAWS mainframe, it performs a *DNS query*. The query represents the workstation “asking” the DNS servers what the TCP/IP address is for a given name. The DNS server responds to the workstation based on the TCP/IP address of record. These records are kept in a database known as the DNS “zone”.

Example DNS

suttera	158.96.xxx.xxx
isaws.cahwnet.gov	158.96.89.78
yahoo.com	66.218.71.198
cisco.com	198.133.219.25

The challenge posed by integrating the ISAWS network is having the county DNS environment and the ISAWS DNS environment support the same workstation. The proper method³ for integrating the DNS records of the state (the HHSDC DNS zone) and the County (county DNS zone) is to perform a zone records transfer. This method has, however, not been approved by HHSDC.

4.1.1 Prescribed DNS Solution - DNS Zone Proxy Server

A DNS zone proxy server consists of Windows NT/2000 Server running DNS proxy server service. An open source DNS solution can also be used.

The service should be setup in a *cache mode only* configuration. The DNS proxy will have no zone configured and will only forward the DNS queries to the state DNS server or the county / ISP DNS server(s). Implementing a DNS proxy allows workstations to be configured with a single DNS server entry, to provide name resolution for state resources and county / Internet resources.

This solution provides dynamic name resolution that does not require manual updates or maintenance. However, it also represents a single point of failure. Failure of the DNS proxy results in a loss of DNS services. Counties with a significant number of

³ Per RFC1035 and RFC1995

workstations may wish to consider multiple DNS proxy servers to balance load and provide fault tolerance.

4.2 IP Routing

As previously stated, counties wishing to configure a hybrid network must install a central network device that can provide NAT translations. This device will perform all TCP/IP packet routing to and from the HHSDC network. Routing within the HHSDC wide area network (WAN) appears to be statically routed, but the static routes are redistributed among the routers.

This means all routes to the various segments of the HHSDC WAN are static routes and these static routes are shared with other routers. However, HHSDC routers do not share the routes with routers not included in the HHSDC routing community, i.e. county maintained routers.

If a given County utilizes routing protocols such as OSPF, IGRP or RIP, and all routes are maintained dynamically, it may not be possible to integrate the HHSDC routing community with the County routing community. From the county routing protocol perspective, the HHSDC WAN is a closed network.

The remaining option available to counties for maintaining routes to and from the HHSDC network segments is utilizing static routes. It is important to identify all HHSDC network segments and the routes needed to reach those segments. Counties configuring a hybrid network should review the ISAWS Consortium document titled "ISAWS-WTW IP Listings¹". This document contains details the ISAWS system resources and the associated TCP/IP address. Using this table, a county can build a routing table on the core router or firewall connected to the HHSDC router, to send all packets destined for the host TCP/IP address to the HHSDC router. To simplify the configuration the routes can be entered into the core router to include destination networks instead of destination segments or hosts.

As per the "ISAWS-WTW IP Listings¹" document, many TCP/IP network segments within HHSDC begin with 158.96 in the first two octets of the network address. Counties can add one route for all networks and segments directing all TCP/IP packets destined for the 158.96.0.0 network to be sent to the HHSDC router. It would not be necessary for the county to enter a route for all TCP/IP traffic destined for a specific ISAWS host, but rather a route to the HHSDC network that the host is connected to. This will greatly simplify the routing tables needed to maintain connectivity to HHSDC resources.

TIP: To simplify routing tables for all HHSDC/ISAWS resources, a county need only configure three general routes⁴. One route to the 158.96.0.0 network,

⁴ Based upon *ISAWS-WTW IP Listings1*

one route to the 169.2.0.0 network, and one route to the 169.3.0.0 network⁵.

NOTE: Counties may wish to filter TCP/IP packets entering the county network for security reasons. However, it is strongly advised that counties NOT filter packets originating from HHSDC to prevent connectivity failures. All ISAWS workstations, printers, DEPCON, and fiscal machines must be reachable from the HHSDC networks for support reasons.

4.3 Netfinity Client

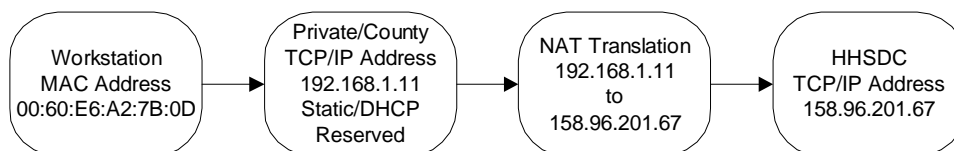
Many counties today no longer utilize the IBM Netfinity client. This client was originally installed on ISAWS workstations to provide remote support from ISAWS System Support. However, this utility is not compatible with Windows 2000 or Windows XP and is no longer supported by IBM. Counties may consider utilizing the VNC utility. See the ISAWS Consortium document titled "WinVNC Remote Support Tool", for additional details.

4.4 Network Address Translation / Port Address Translation

NAT/PAT is the component required to provide transparent connectivity to HHSDC. Each ISAWS machine will need to be statically addressed. This can be accomplished manually or dynamically using DHCP (Dynamic Host Configuration Protocol) reservations (based on the MAC address) using the county's internal private addressing scheme. These private addresses would then be translated to static HHSDC assigned addresses.

The ISAWS host mainframes require static TCP/IP addressing for some devices such as printers but will allow PAT addressing for workstations.

Below is the logical flow of the workstation addressing



Please refer to the **CTS – Hybrid Network NAT/PAT guide** for additional information.

4.5 ISAWS Supported Email

ISAWS email accounts are provided to some county staff. These email accounts are hosted on an Exchange server (HHSIEXMB01) located at HHSDC. The Exchange server presents a challenge to counties configuring a hybrid network, in that the server

⁵ Subnet mask: 255.255.0.0 or /16 to specify the first two octets as the network portion of the packet header

will be accessible from both the internal network (Private county LAN to HHSDC WAN) and the Internet. This results from the mail server (HHSIEXMB01) being reachable from both the internal network and by the Internet.

Because HHSDC uses the same TCP/IP address on both the internal network and the external network (Internet) a routing loop is created. HHSDC blocks Exchange accounts from connecting to the Internet. Having IP addresses available from both the closed network as well as the Internet poses a complex routing issue for the counties.

Having these types of routing loops can cause difficulties when sending and receiving certain types of e-mail. Most counties switch to a county e-mail address when they move to a hybrid network environment. HHSDC can setup e-mail forwarding from the ISAWS accounts to the new county accounts, so that counties can continue to receive e-mail from their ISAWS accounts.

UPDATE: ISAWS email hosting services have been transferred to HHSDC. The impact of this change has not yet been evaluated.

4.6 Timed Out Connections (EU Screen Recovery)

Counties that integrate ISAWS into the county network should perform a pilot connectivity test to verify that issues with the central connection to HHSDC do not exist.

As a result of how MAPPER tracks incoming connections on the ISAWS mainframes, connection “time out” values should be set to never time out, or time out at the greatest value possible. If a connection is dropped for any reason (i.e. connection time out, equipment failure, broken cable, etc.) the End User (EU) screen will be left open on the mainframe, commonly referred to as a “hung” screen. Once this occurs the screen must be manually reset, in order to open the EU screen. This is much the same as an AS/400 session.

Serious problems may arise if the connection to HHSDC is dropped while all ISAWS connections are being routed through the central router or firewall connection. If the central connection is dropped, EU screens can potentially be left open on the mainframe.

In the event of a mass connection failure (the central connection is lost) there is a process to get all of the EU screens reset. This process can take as long as a few days in some cases. The process consists of recording all of the hung EU screens and submitting this list as an emergency Remedy ticket.

TIP: Counties may wish to create a spreadsheet listing all EU screens.

NOTE: ISAWS System Support staff prefer to have all screens listed in the ticket to allow for pasting to the application that resets the screens, which may

expedite the process. The alternative is to request that ISS reboot the box the county is connected to during the maintenance window of 11:00pm to 2:00am. This is considered a last resort recovery process.

5.0 DEPCON and Fiscal Workstations

Some counties may have special concerns about the DEPCON and fiscal ISAWS workstations. These machines may be integrated into the county network the same as the standard ISAWS workstations. Some counties may also choose to leave these machines directly connected to the HHSDC network if feasible.

Requirements for DEPCON and fiscal workstations are the same, as other ISAWS workstations. The central router or firewall connected to the HHSDC network will need to allow incoming ftp connections to the DEPCON machine, for the nightly print runs to occur. As previously stated, counties are strongly advised NOT to filter incoming packets from the HHSDC networks this will effect ISAWS support staff's ability to remotely support the DEPCON and fiscal workstations.

Change Control Log

Version	Change	Editor	Date
0.0			