INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Intended for Information Technologies Professionals, this document serves as a single source for all technical requirements related to the configuration and use of labor management solutions provided by Lone Wolf Software, Inc. dba Inception Technologies.

Table of Contents

Technical Requirements Listed by Employee Count

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Employee Count	0-250	250-500	500-2000	2000+
Concurrent Connections	10	50	100	100+
RAM	8 GB	8 GB	16 GB	16 GB +
Hard Drive Space	10 GB Free	20 GB Free	50 GB Free	100 GB Free
Bandwidth	100 Mb/s for LAN Cable or DSL for WAN	100 Mb/s for LAN Cable or DSL for WAN	1 Gb/s for LAN Cable or DSL for WAN	1 Gb/s for LAN Cable or DSL for WAN
Processor Speed	Quad Core Processor (Intel Xeon, I5, I7 or equivalent.) 2.0 Ghz or Higher	Quad Core Processor (Intel Xeon, I5, I7 or equivalent.) 2.0 Ghz or Higher	Quad Core Processor (Intel Xeon, I5, I7 or equivalent.) 2.4 Ghz or Higher	Quad Core Processor (Intel Xeon, I5, I7 or equivalent.) 2.4 Ghz or Higher
Operating System	Windows 7 Professional or Ultimate Edition 64-bit Win 2008 Server 64 bit	Win 2008 Server Standard or Enterprise Edition 64-bit	Win 2008 Server Standard or Enterprise Edition 64-bit	Win 2008 Server Standard or Enterprise Edition 64-bit
Storage System	Single Disk	Two Single Disk Drives Recommended: One for the OS and one for the Database	RAID 5 or RAID 10	RAID 5 or RAID 10

Technical Notes & Exclusions:

- Inception Technologies does not support installations of InfiniTime on Domain Controllers or servers with Microsoft Exchange 2007/Microsoft Exchange 2010 installed.
- InfiniTime does not support installation on any Home version of Windows.
- Inception Technologies does not provide support for the configuration of customer network architecture or the configuration of a virtual server and related storage solutions. Support will be provided for Virtual Machines hosted exclusively on the VMWARE platform under the following conditions:
    - The virtual machine must meet the minimum hardware and operating system requirements.
    - The InfiniTime Database must not be installed on a virtual hard disk. Physical storage must be made available to the virtual operating system through use of Direct Attached Storage (DAS) or a Storage Area Network (SAN).

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

InfiniTime Server Requirements

In order for client machines to access the InfiniTime Server the following ports must be open to all inbound traffic. Any hardware or software firewalls in the customer's environment must be configured to pass traffic on these ports to the InfiniTime Server.

Port	Protocol	Purpose
80	TCP	HTTP Access to InfiniTime Web Site
443	TCP	HTTPS Access to InfiniTime Website
21	TCP	FTP Access to InfiniTime Input and Output FTP Sites
1521	TCP	Oracle Listener – Must be open for connections to the InfiniTime Database.

Additional InfiniTime Server Requirements and Concerns

- If the InfiniTime Application is published to the Internet secure communications (HTTPS) are recommended for security purposes.
- Standard Information Technology practices dictate that Domain Controllers remain free of additional applications. Inception Technologies strongly recommends against the installation of the InfiniTime Application on a Domain Controller.
- When possible InfiniTime should be installed on a stand-alone server free of other Enterprise Applications such as SQL Server Enterprise Edition. If no other options are available an additional 2 GB of RAM beyond the Minimum Requirements of the Operating System and InfiniTime Application are recommended, though additional RAM may be required depending on the exact applications running on the InfiniTime Server.
- When possible InfiniTime should not be installed on a server with Sharepoint. Inception Technologies does not provide support for Sharepoint Setup or configuration. Sharepoint listens for and receives all incoming HTTP Requests to the InfiniTime server which can stop InfiniTime from operating properly. Customer's who choose to install InfiniTime on a server with Sharepoint are responsible for configuring Sharepoint to allow users to access the InfiniTime Website.
- InfiniTime should not be installed on a server with Microsoft Exchange 2007 or Microsoft Exchange 2010. Microsoft Exchange 2007 and 2010 are not compatible with 32-Bit Web Applications with a default Exchange installation. Customers who choose to install on a server with Microsoft Exchange 2007 or 2010 acknowledge that Inception Technologies does not provide support for this configuration and accept responsibility for manually configuring their Server Environment to support 32-Bit Web Applications. Additional information can be found at the following Microsoft Knowledgebase articles and web links:

  http://forums.iis.net/p/1154189/1890537.aspx
  http://technet.microsoft.com/en-us/library/bb124035(EXCHG.65).aspx
  http://technet.microsoft.com/en-us/library/aa996644(EXCHG.65).aspx

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Installation Summary

Pre-Installation

- **Minimum Requirements**: Please ensure your chosen server for the InfiniTime software meets the minimum hardware and software requirements as specified in the Installation Manual. Note that Internet access is required during installation in order to register certain aspects of the software in preparation for normal use.
- **Windows Updates**: Please check Windows Update and install all recommended updates prior to installing InfiniTime 7.0
- **Windows Logon Security**: If you plan to join the InfiniTime 7.0 Server to a Domain this task must be performed before installation. If your computer is already joined to a Domain then installation must be performed while logged into the Domain Administrator Privileges.
- **Windows Console Session**: Installation must be performed while logged onto the console session. Do not attempt to use Remote Desktop to install InfiniTime.
- **Data Execution Prevention**: Data Execution Prevention must be disabled within Windows XP Pro SP2 and Windows 2003 Server before proceeding with the installation.
- **Windows Firewall**: Windows Firewall must be disabled during the installation process. Please disable Windows Firewall before proceeding with the installation.
- **Personal Firewall Software**: Personal Firewall Software must be disabled during the installation process. Please disable any Personal Firewall Software such as Norton Personal Firewall or Zone Alarm Pro before proceeding with the installation.
- **Antivirus Software**: Antivirus software must be disabled during the installation process. Please disable any Antivirus software before proceeding with the installation.
- **Windows Operating System CD**: Your Windows Operating System CD may be required during installation. Please have it handy.
- **Check for Internal/Built In Modem**: If your installation will include direct connect clocks, verify that you do not have a modem sharing resources with the com port that will be utilized for the clocks.

Installation

- **Starting the Installation**: To start the setup wizard insert the InfiniTime 7.0 Program Disk into your CDROM drive. Open my computer and browse to the CD. Run setup.exe
- **Installation**: Follow the onscreen instructions during the installation process. Please refer to the Installation Manual for detailed screen by screen instructions.
- **Program & Data Directories**: InfiniTime Program and Data directories must reside on the InfiniTime server on a local hard drive and may not be placed on a remote network or mapped drive.

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Post Installation

- **Software Key**: The software key included with your InfiniTime 7.0 software contains your software licensing information. Do not misplace this software key. Please insert your software key into the InfiniTime 7.0 server once the software installation is complete.
- **Backup Software Configuration**: Should backup utilities such as Windows XP Professional System Backup or VERITAS be utilized on the InfiniTime server they must be configured in order to prevent damage to the InfiniTime Database. Be sure to exclude the InfiniTime Installation Directory, Data Location, and C:\Program Files\Oracle from being archived by these utilities.
- **Antivirus Software Configuration**: Antivirus software must be configured to exclude the InfiniTime Installation Directory, Data Location, and C:\Program Files\Oracle from routine scans in order to prevent damage to the InfiniTime Database.
- **Data Execution Prevention (OPTIONAL)**: Data Execution Prevention **may** be re-enabled after the installation process, however exceptions must be configured. Refer to the Installation Manual for more details.
- **Pop Up Blockers** – Pop Up blockers must be disabled or configured to allow pop ups from the InfiniTime server. This includes the native Internet Explorer Pop Up blocker in addition to those included with add-ons such as Google Toolbar.
- **Windows Firewall & Software Firewalls**: Windows Firewall and Personal Firewall Software may be re-enabled after the installation process, however exceptions must be configured. Refer to the Installation Manual for more details.
- **Read the Quick Start Guide**: The InfiniTime Quick Start Guide is designed to assist first time users with navigating the software interface and basic system configuration. The Quick Start Guide can be viewed within the electronic help system or as a PDF file. Simply insert the resource disk and click on the Documentation button to access the InfiniTime Manual in PDF Format.

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

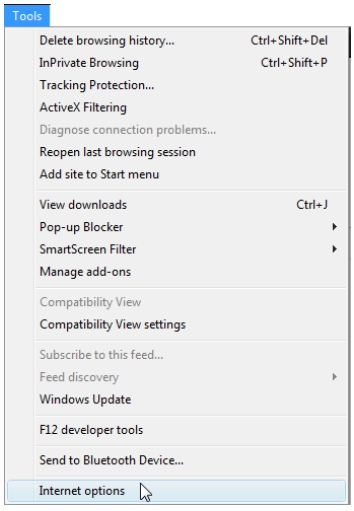
InfiniTime Labor Management Systems

Client Machine Configuration

As a Web Application, InfiniTime 7.0 uses a Web browser to display the interactive portions of the software. Certain security features and settings must be set properly in order for InfiniTime 7.0 to display correctly and to permit printing from InfiniTime 7.0 on a Client machine. The URL used to access the InfiniTime Software will be referred to as the InfiniTime 7.0 Web Address throughout this section. Internet Explorer must be configured as listed below for all client machines. Instructions are provided for Internet Explorer 8 (IE8) and Internet Explorer 9 (IE9).

Required Browser Configuration for IE 8:

1. Add the InfiniTime 7.0 Web Address as a Trusted Site
    a. Click on the Tools menu, then click on Internet Options



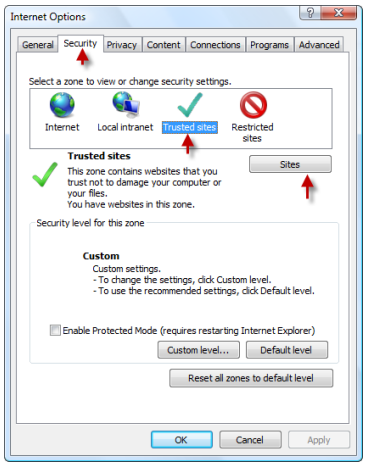
    b. Click on the Security Tab on the Internet Options Menu then click on Trusted Sites to highlight it. Click on the sites button to see current Trusted Sites.

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

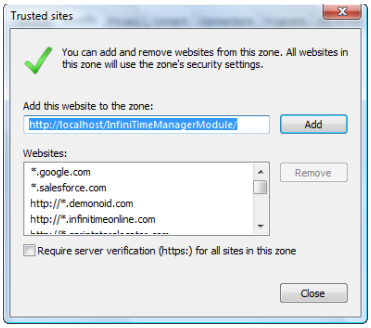
www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems



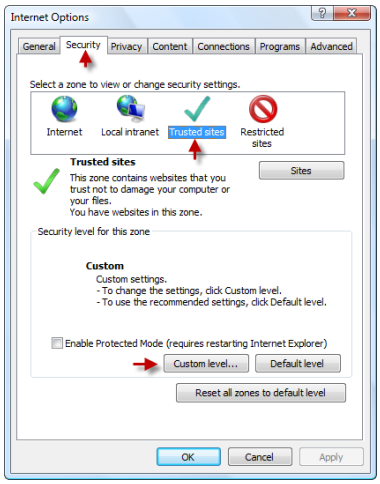
c. Type the InfiniTime 7.0 Web Address then click Add



Information Technologies Brief

InfiniTime Labor Management Systems

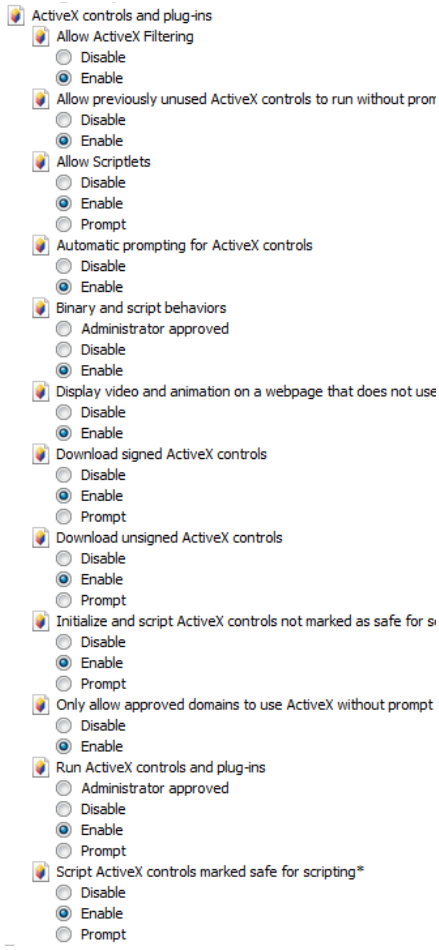
2. Configure Required Active-X Controls for the Trusted Sites Zone
    a. Click on the Security Tab on the Internet Options Menu then click on Trusted Sites to highlight it. Click on the Custom Level button to view current Active-X Control settings.



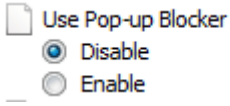
Information Technologies Brief

InfiniTime Labor Management Systems

b. In the Security settings for the Trusted Sites Zone confirm the Active-X controls are configured as shown below.



c. Additionally, in the Security Settings for the Trusted Sites Zone, ensure the Pop-Up Blocker is disabled.



INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

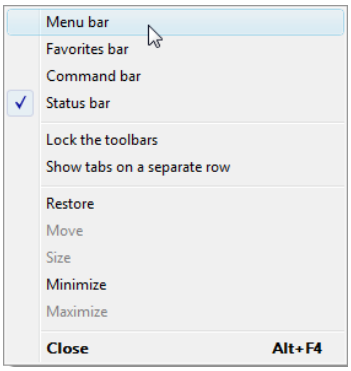
www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

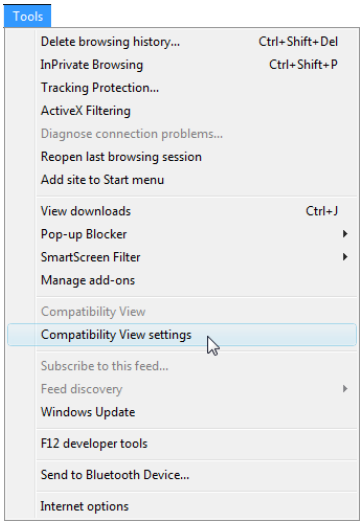
InfiniTime Labor Management Systems

Required Browser Configuration for IE 9:

1. Enable Compatibility Mode
    a. Right click on the status bar and check the option Menu Bar



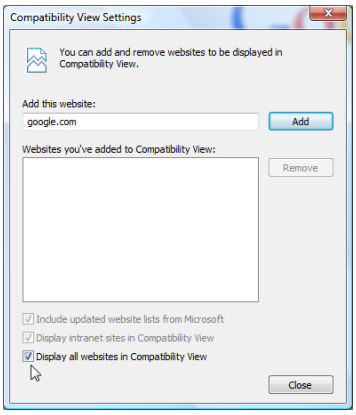
    b. Click on the Tools menu, then click on Compatibility View Settings



Information Technologies Brief

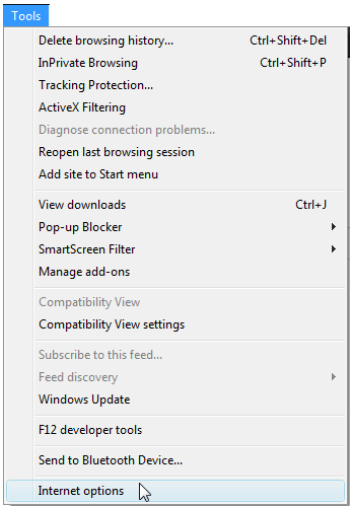
InfiniTime Labor Management Systems

c. In the Compatibility View Settings check the option to Display all Websites in Compatibility Mode, then click on Close.



2. Add the InfiniTime 7.0 Web Address as a Trusted Site

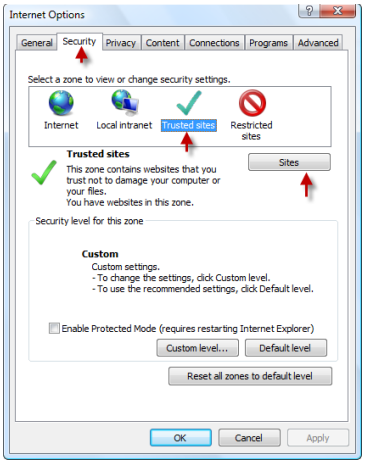
a. Click on the Tools menu, then click on Internet Options



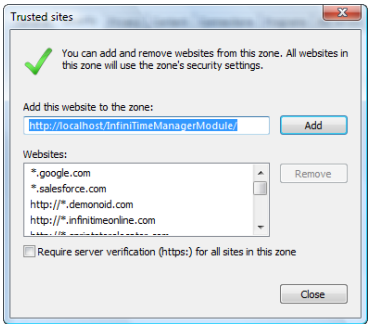
Information Technologies Brief

InfiniTime Labor Management Systems

b. Click on the Security Tab on the Internet Options Menu then click on Trusted Sites to highlight it. Click on the sites button to see current Trusted Sites.



c. Type the InfiniTime 7.0 Web Address then click Add

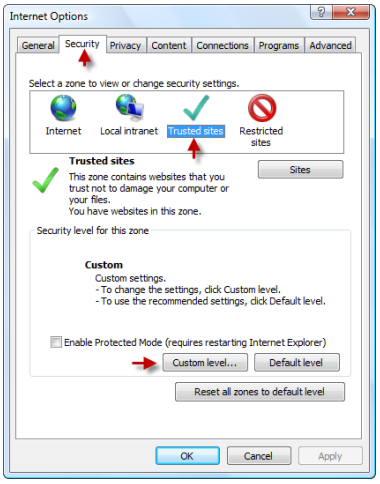


Information Technologies Brief

InfiniTime Labor Management Systems

3. Configure Required Active-X Controls for the Trusted Sites Zone

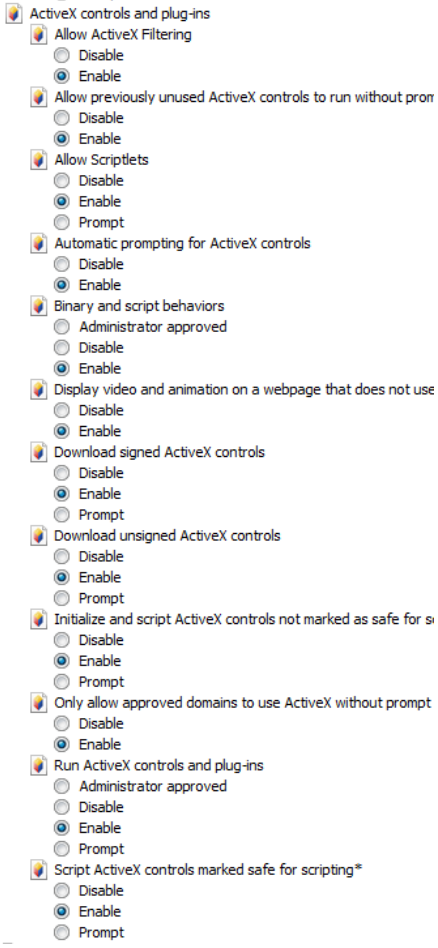
    a. Click on the Security Tab on the Internet Options Menu then click on Trusted Sites to highlight it. Click on the Custom Level button to view current Active-X Control settings.



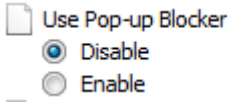
Information Technologies Brief

InfiniTime Labor Management Systems

b. In the Security settings for the Trusted Sites Zone confirm the Active-X controls are configured as shown below.



c. Additionally, in the Security Settings for the Trusted Sites Zone, ensure the Pop-Up Blocker is disabled.



INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Minimum Requirements for TCP/IP Clocks

In order to effectively ensure communication from the software to the time TCP/IP Time clock it is important to ensure that the correct protocols and ports are available. Default Ports and Protocol Requirements are listed below for each Hardware Terminal. Your equipment must be configured to permit traffic to these ports via direct LAN Communication or via Port Forwarding or Network Address Translation for Remote Ethernet Terminals.

NOTE: Please refer to the "Ethernet Hardware Terminals: Configuration Scenarios for Remote Sites" for more information about configuring Ethernet Readers for access over the Internet.

Reader Type	Default Port	Protocol
Athena	4370	UDP
Juno	4370	UDP
Luna	4370	UDP
Scout 1000 / 2000 / 3000 / 4000	3001	TCP
Thor	4370	UDP
Zephyr	4370	UDP

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Alternate Communication Methods – Requirements

If your terminals (or other hardware) will use TCP/IP communication, please reference the below information and the requirements for each piece of hardware and communication method. Requirements are listed below for Alternate Communication Methods such as Modem, Cellular, and Telephone Punch. Customer equipment must meet these requirements to be supported.

Communication Method	Requirements
Telephone Punch	• Dedicated Analog Phone Line at InfiniTime Server • Caller ID Services must be provided for the Dedicated Analog Phone Line • Dialogic Media Board of appropriate Form Factor (PCI / PCIe) Purchased from Lone Wolf Software, Inc. • Envox 6 Console Application Purchased from Lone Wolf Software, Inc. • Supported Operating Environment: Windows XP Professional or Windows 2003 Server only
VISTOR (Wireless G Access Client)	• 802.11b or 802.11g Wireless Network and Wireless B or G Gateway • 2 Available Internal Static IP Addresses • Ability to configure Network Address Translation or Port Forwarding for remote clocks. An available public IP Address will be required at the remote site for Network Address Translation • Knowledge of Wireless Network Configuration (IE: Wireless SSID, Wireless Security Type, Wireless Security Settings)
Cellular	• A Supported USB Cellular Modem with an active Cellular Data Plan. (See Appendix A) • Ideally, the USB Cellular Modem should be assigned a Static IP Address. Otherwise Dynamic DNS Must be configured for the USB Cellular Modem. • A computer with an Ethernet NIC.
Modem	• External V.92 Modem. Internal WIN Modems are not supported. • Dedicated Analog Phone Line at InfiniTime Server • Dedicated Analog Phone Line at Modem Clock

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Access Control Requirements

Access Control offers customers the ability to control employee access to facilities. Only specific hardware terminals offered by Inception Technologies provide support for Access Control. Only the InfiniTime Product Line supports Access Control Functionality.

Hardware Terminals with Support for Access Control

Reader Type	Max # of Independently Controlled Entryways
Athena	1
Thor	2
Scout 3000	1
Scout 4000	1

Additional Access Control Requirements and Concerns

- Access Control Functionality requires purchase of the Access Control Software Module for InfiniTime 7.0
- Wiring is the responsibility of the customer. Improper wiring may result in damage to equipment and is not covered under warranty.

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Bell Scheduling Requirements

Bell Schedules offer customers the ability to sound a bell at predefined intervals. Two hardware options are available for bells. Internal bells play a bell sound on the clock itself and are intended for small offices. External bells use a relay to active a buzzer or bell system and are intended for large buildings or warehouses. Only specific hardware terminals offer support for Bell Scheduling.

Hardware Terminals with Support for External Bells

Reader Type	Max # of Bell Schedules
Athena	
Thor	1024
Scout 3000	
Scout 4000	

Hardware Terminals with Support for Internal Bells

Reader Type	Max # of Bell Schedules
Athena	
Thor	1024
Luna	
Zephyr	

Additional Bell Scheduling Requirements and Concerns

Bell Scheduling Functionality requires purchase of the Bell Scheduling Software Module for InfiniTime 7.0

Wiring is the responsibility of the customer. Improper wiring may result in damage to equipment and is not covered under warranty.

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Security Applications: Firewalls and Antivirus

InfiniTime performs multiple functions which require a certain level of access to resources on the InfiniTime Server and on the local network. Security Applications Such as Firewalls, Antivirus, and Security Suites such as Norton Internet Security must be configured correctly in order for InfiniTime to operate. Configuration of Firewall and Antivirus software is the responsibility of the customer.

Firewall Software

Firewall Software Applications protect the host computer by blocking network traffic and by prohibiting applications from accessing the network. Firewall applications must be configured to permit outbound access to the local network as needed. Oracle.exe must also be added as an exception to the Firewall. All network traffic inbound or outbound from Oracle.exe must be permitted. The default location of Oracle.exe is listed below according to product.

InfiniTime 7.0 C:\Inception\InfiniTime\Ora10\bin\oracle.exe

Software Firewalls installed on the InfiniTime Server must be configured to permit inbound traffic on the following ports:

Port	Protocol	Purpose
80	TCP	HTTP Access to InfiniTime Web Site
443	TCP	HTTPS Access to InfiniTime Website
21	TCP	FTP Access to InfiniTime Input and Output FTP Sites
1521	TCP	Oracle Listener – Must be open for connections to the InfiniTime Database.

Antivirus Software

Antivirus Software actively searches computer hard drives and removable drives comparing files and their contents against a database of known viruses. Antivirus programs generally advance through the file structure of a hard drive file by file, accessing each and inspecting it in turn. This operation can interfere with the function of the Oracle Database used by InfiniTime. As a security measure Oracle Databases will shut themselves down when their files are improperly accessed. Antivirus Software must be configured with exceptions for InfiniTime and Oracle files in order to avoid potential conflicts with the Oracle Database. Exclusions are listed below by product type.

InfiniTime 7.0

InfiniTime Installation folder - Default Location is: C:\Inception\InfiniTime\
Oracle Program Files – Default Location is: C:\Program Files\Oracle

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Additional Security Application Related Concerns

- InfiniTime performs automated functions and can be configured to Email reports to supervisors or employees as needed. Some antivirus or security suites block outgoing email. It may be necessary to configure additional settings in order to permit outbound email from InfiniTime. Steps for permitting outbound email differ from application to application. Consult documentation for the Security Application if needed.

Accessing the InfiniTime Application – Supported Browsers

As of InfiniTime 7.06c the following browsers are supported:

Internet Explorer 7
Internet Explorer 8 (Compatibility Mode)
Internet Explorer 9 (Compatibility Mode)
Firefox
Safari

Attempting to access and utilize the InfiniTime Application from alternate browsers may result in script errors.

Pop Up Blockers & Toolbars

Many Internet Explorer toolbars include their own pop-up blocker. These must be disabled or configured to allow pop-ups from http://localhost/ on the server machine. Failure to disable pop-up blockers will cause InfiniTime 7.0 to display improperly. Generally the user will be unable to login to the software itself.

The most popular Internet Explorer tool bars include:

Google Toolbar
Yahoo Toolbar

Instructions for use and configuration of these products can be found at the developer's website as listed below.

Google Toolbar Support:
http://www.google.com/support/toolbar/

Yahoo Toolbar Support:
http://help.yahoo.com/l/us/yahoo/toolbar/features/popupblocker/index.html

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Supported USB Cellular Modems (Sorted by Carrier)

ALLTEL
- Huawei EC228
- Huawei EC168
- UTStarcom UM150 (a.k.a. Pantech UM150)
- UTStarcom UM175 (a.k.a. Pantech UM175)

CRICKET
- Calcomp a600
- UTStarcom UM100 (a.k.a. Pantech UM100)

NTELOS
- Franklin CDU-680

SPRINT (3G)
- Franklin CDU-550
- Franklin CDU-680
- Franklin U300
- Novatel U720
- Novatel U727
- Novatel U760
- Sierra Wireless 595U
- Sierra Wireless 597U (Compass 597)
- Sierra Wireless 598U

T-MOBILE
- Huawei E181 (a.k.a. WebConnect USB Laptop Stick)

VERIZON
- Novatel USB720
- Novatel USB727
- Novatel USB760
- Sierra Wireless 595U
- UTStarcom UM150 (a.k.a. Pantech UM150)
- Pantech UM175

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Ethernet Hardware Terminals: Configuration Scenarios for Remote Sites

Terms:

Protocol - One way to think about and understand the purpose of a protocol is to compare it to a standard. People throughout the world work in different languages, on different types of machines, using different software applications, and different types of computers. As a whole it would not be possible for worldwide communication to occur without certain standards governing how information can be exchanged between different groups or individuals. These standards for communication can be described as a set of rules. Similarly there are also rules for governing how data is sent over a computer network which are referred to as protocols. For example the Internet Protocol, often referred to as IP, defines how packets of information are transferred across the internet.

IP Address - Each computer on a network is assigned an IP Address in order to communicate with other machines. This idea can be illustrated by comparing a network to a town. Each building in a town is identified by a street address. If a building did not have a street address it would not be possible to locate it or provide instructions for others to travel to it. Similarly every computer on a network must have an IP address in order to communicate with other machines on the network. IP Addresses have four parts which are referred to as an octet. Each octet is separated by a period as shown below. Valid values for each octet include 0 to 255.

192.168.0.10

First Octet Second Octet Third Octet Fourth Octet

Static IP Address - A static IP Address is assigned to an individual and does not change. Returning to the Network : Town analogy this can be compared to a building which is always found at the same street address. This makes it possible for others to always know where the building, or a computer in the case of a network, is found. Businesses that provide a service to the community make their street address public in order for customers to be able to find them. Similarly computers that provide a service are generally assigned a static IP Address in order to ensure remote computers will be able to find and communicate with them.

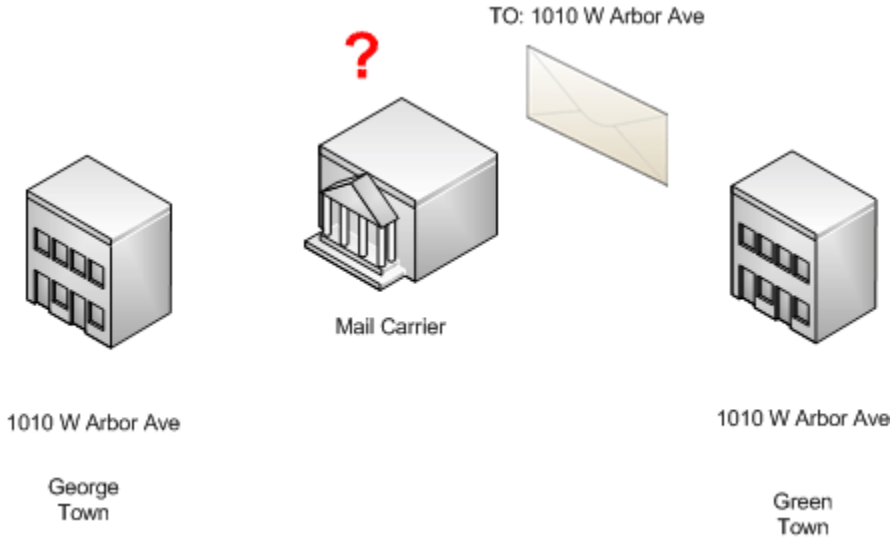
Dynamic IP Address - A dynamic IP address is assigned to an individual on a temporary basis. Returning to the Network : Town analogy this can be compared to a street cart which will not always be located at the same spot in the town. It would not be possible for an individual to find the street cart without having prior knowledge of its location or an alternate method of contacting them. Similarly it is not possible for a computer with a dynamic IP Address to provide services to other computers on a network without using additional services such as a Domain Name System (DNS) or a Dynamic Domain Name System (DDNS) to provide an alternate means of identification.

Internal // Private IP Addresses - An Internal IP Address refers to an IP Address which is only valid inside of a private network. Unlike Public IP Addresses internal IP Addresses are specifically set aside for use on private networks and can be used by anyone. This means that three networks, or even three million networks, can each use the same Private IP Addresses. Returning to the Network : Town analogy

Information Technologies Brief

InfiniTime Labor Management Systems

if we think of our town as a small part of a larger city we begin to understand this concept as is not uncommon for a street to have the same name in different towns. A street address for a specific building in the town only refers to that specific building inside of that town. Similarly an Internal IP Address is only valid inside of a private network. Lets break down this example into a bit more detail. The image below shows two buildings with a street address of 1010 W Arbor Ave. Each building is located in a different town. A mail carrier responsible for delivering mail to each of these buildings receives a letter postmarked to 1010 W Arbor Ave. Anyone specifically located in George Town or Green Town would know where 1010 W Arbor Ave is. Yet to the rest of the world there is no way to determine which building the letter is intended to be sent to without additional information. For our town this additional information would take the form of City, State, Zip which tells us where in the world the specific street address is located. On a network a packet of information would be forwarded to a Public IP Address where it is then forwarded to the correct Internal IP Address. The network diagram below shows three computers each on a different private network. Two of the private networks use the same Internal IP addresses for their computers. It is not possible for the Host B to send information to Host A using its Private IP Address. Private IP Addresses cannot be used to communicate on the Internet.

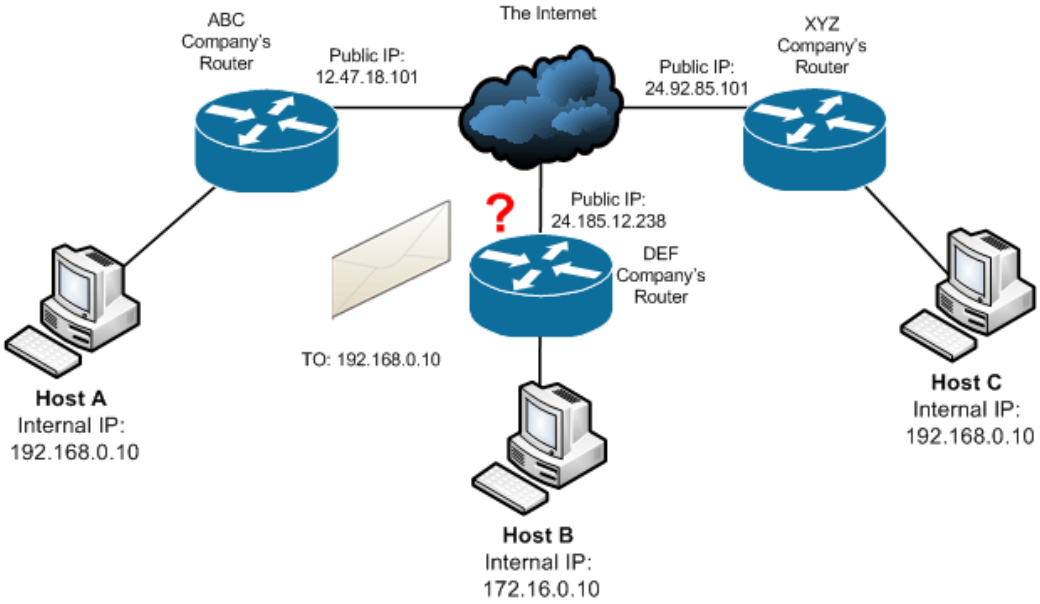


INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems



The following are valid internal IP Address ranges. Remember an IP Address consists of four octets with valid values of zero to two hundred and fifty five (0 - 255) Any IP Address that falls within these ranges is an internal IP Address and cannot be used to communicate on the internet. In some cases you may be accidentally provided with an IP Address that falls within one of these ranges for an Ethernet clock at a remote site. The address you have been provided is the Internal IP Address for the clock on the remote network and is not the correct information. Remember internal IP Addresses cannot be used to communicate across the internet. Please request the Public IP Address for the remote site. This is the address you will need to setup within InfiniTime to communicate with your remote Ethernet clock. Refer to the scenarios below for more information.

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

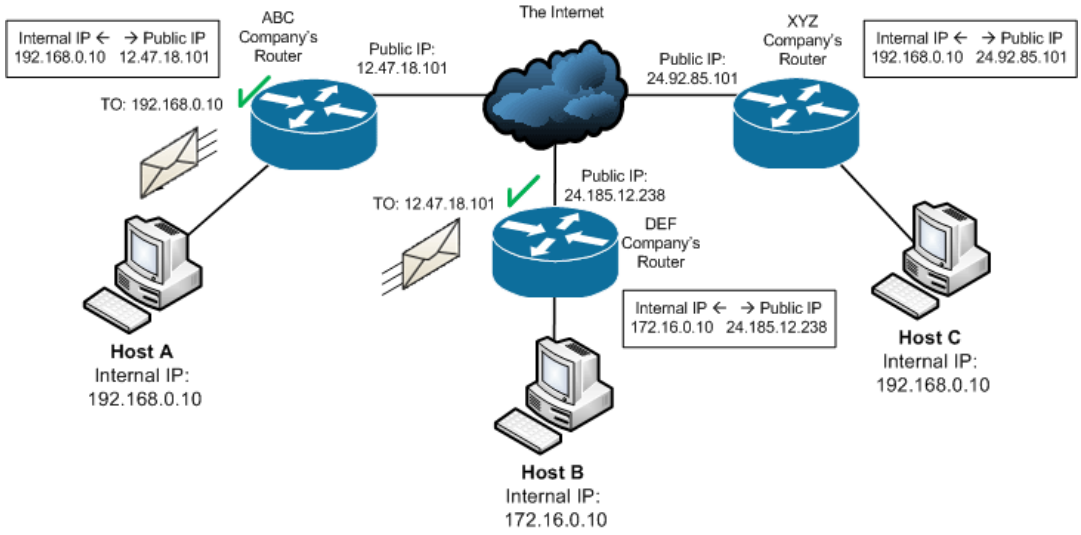
192.168.0.0 - 192.168.255.255

Public IP Address - A Public IP Address refers to an IP Address which is used to communicate with other computers and devices on the Internet. Pubic IP Addresses are registered with a Regional Internet Registry (RIR) to avoid addressing issues. Only the registered holder of a Public IP Address can assign the address to a network device for communication on the Internet. Returning to our Network : Town analogy the City, State, and Zip Code help to identify where a specific street address is located within the world. Similarly a Public IP address specifies a computer's location on the Internet. Remember, Internal IP Addresses cannot be used to communicate on the Internet. For this reason a method must exist to translate between Internal IP Addresses and Public IP Addresses in order for hosts on a private network

Information Technologies Brief

InfiniTime Labor Management Systems

to communicate on the Internet. Network Address Translation (NAT) and Port Address Translation (PAT) provide this service. The image below shows traffic flow from Host B to Host A.



Port - The best way to understand the role of a port in network communication is to return to our Network : Town analogy. Each building in a town has a specific street address which from our earlier examples is comparable to an IP Address. Each building also has multiple doors or points of entry from the outside world which are comparable to ports. Just like a door on a building makes it possible for multiple people to walk in and out of the building at once, ports make it possible for multiple conversations with other network devices or applications to occur simultaneously. Also similar to a door, a port can be in a closed or open state. A closed port does not have a service listening for traffic behind it. Any communication sent to a closed port will not reach the end destination successfully as illustrated below. Each port on a computer is identified by a port number. Port numbers range from 0 to 65535. Different applications and network services use different ports.

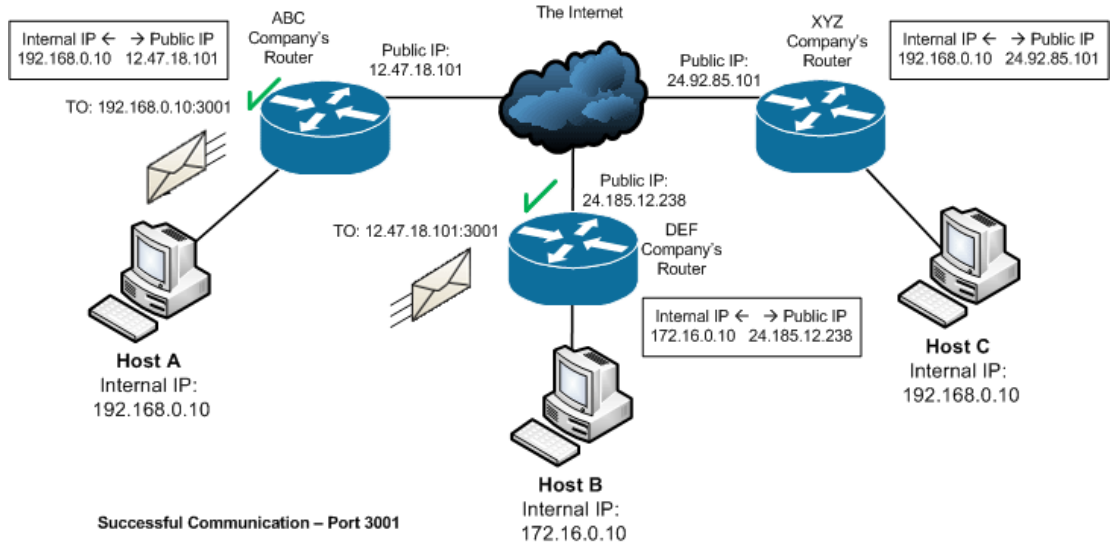
INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

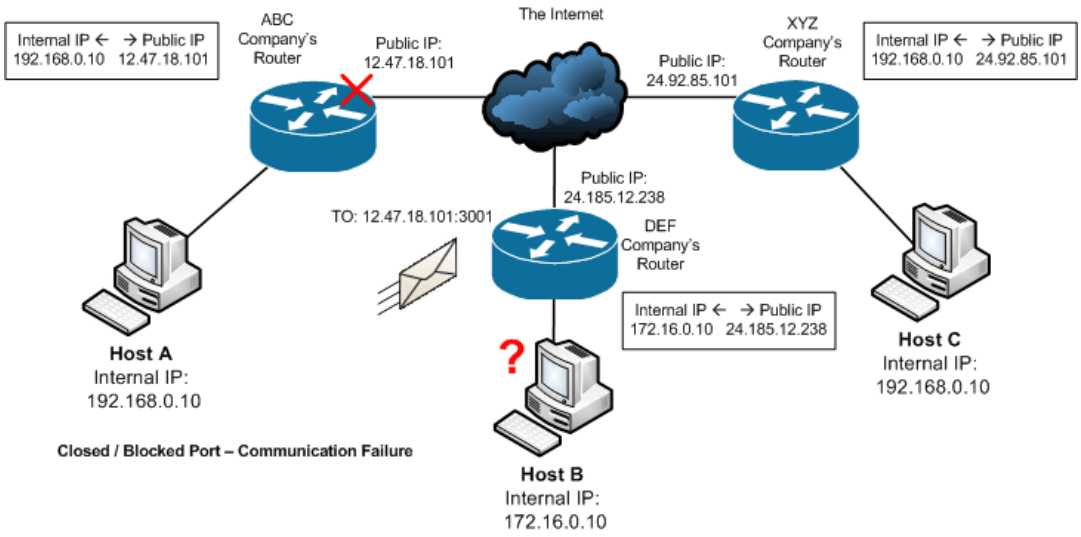
Information Technologies Brief

InfiniTime Labor Management Systems

Successful Communication – Port 3001:



Closed / Blocked Port – Communication Failure:



INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

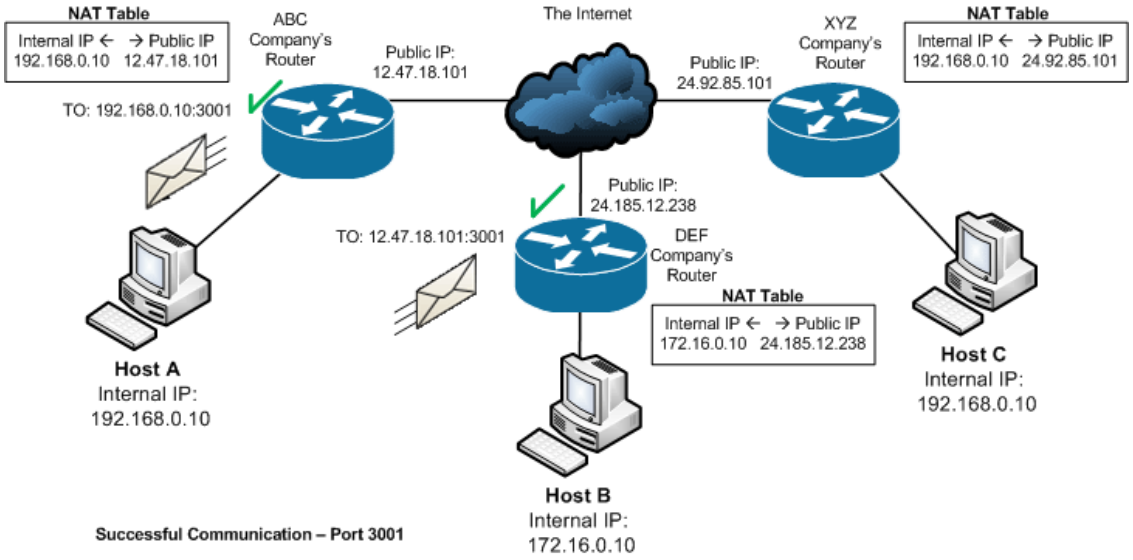
Information Technologies Brief

InfiniTime Labor Management Systems

TCP & UDP - Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are two protocols or sets of rules which govern how traffic is sent between ports on a network. It is important to understand that a device expecting TCP data on a specific port will not function if the data is sent with UDP instead, though some devices will support both. A list of the Ethernet Clocks offered by Inception Technologies are listed below along with the port and protocol used by the clock.

Manufacturer	Model	Port	Protocol
Schlage	Scout 1000, 2000, 3000 & 4000	3001	TCP
ZK Software	Athena	4370	UDP
ZK Software	Juno	4370	UDP
ZK Software	Thor	4370	UDP
ZK Software	Luna	4370	UDP
ZK Software	Zephyr	4370	UDP
Synel Industries	Apollo 715	3734	TCP or UDP
Synel Industries	Atlas 777	3734	TCP or UDP
Synel Industries	Orion 760 & Odyssey 780	3734	TCP or UDP
Synel Industries	Omega 755	3734	TCP or UDP

Network Address Translation (NAT) - As mentioned above NAT provides a mechanism for translating between Internal and Public IP Addresses. Without NAT it would not be possible for computers or devices on a private network to communicate across the internet. The image below shows successful communication between Host B and Host A. The NAT Table for each router is also shown to illustrate how an Internal IP Address is mapped to a Public IP Address. Though multiple methods exist for mapping Public IP Addresses to Internal Addresses, a static NAT mapping is generally used for configuring an Ethernet clock at a remote site. A static NAT mapping is used to map a specific Public IP Address to a specific Internal IP Address. In this way the internal device can always be reached at a specific public address. The example below illustrates NAT mappings as each internal device will always be assigned the same Public IP Address.



INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Port Address Translation (PAT) - As mentioned above PAT provides a mechanism for translating between Internal and Public IP Addresses. PAT uses ports to map multiple Internal IP Addresses to a single Public IP Address. This type of Address Translation cannot be used to forward network traffic directly to an Ethernet Time and Attendance terminal. Port Forwarding must be used in conjunction with PAT in order to establish communication.

Domain Naming System (DNS) - Domain names of popular websites such as Google or Microsoft may be familiar to you already. DNS maps a word or phrase to an IP Address in order to make it easier for people to remember how to get to a website or computer on the Internet. DNS is considered an essential network service and is required to access a website or computer on the internet using a domain name. It is important to note that DNS maps a single IP Address to a single domain. For this reason most domains are mapped to a static Public IP Address.

Dynamic Domain Naming System (DDNS) - In some cases it is not possible to obtain a Static Public IP Address. This is often the case when using a non-commercial Internet Service such as residential DSL or Cable as many Internet Service Providers (ISP) will not provide a Static Public IP Address for these connection types. If a Static Public IP Address is not available Dynamic DNS (DDNS) must be used to map your Public IP Address to a DDNS domain. The dynamic DNS domain can then be used to communicate with devices on your network. Dynamic DNS is provided as a service and is available for free from many sources online. Use your preferred search engine to perform a search for 'free dynamic dns' to find free DDNS providers. Your router must support DDNS in order to use it. Not all routers support this service.

Internet Service Provider (ISP) - An Internet Service Provider is a company that collects a monthly or yearly fee in exchange for providing subscribers with Internet Access. Internet Services vary in price, speed, and service type. Various services are available depending upon your area. Dial up, DSL, and Cable, are common non-commercial services though Dial up has largely become outdated except in rural areas where other services are not available. It should be noted that some ISPs will block certain port ranges in an attempt to provide security. To prevent possible difficulties it is good practice to contact your ISP in order to determine what, if any, ports are being blocked.

Router - A router is a device that is responsible for forwarding data packets from one network to another. It is important to note not all routers are the same as their role differs from network to network. When working with remote Ethernet clocks it is important to ensure support for the following features is available: NAT, Port Forwarding, and Dynamic DNS.

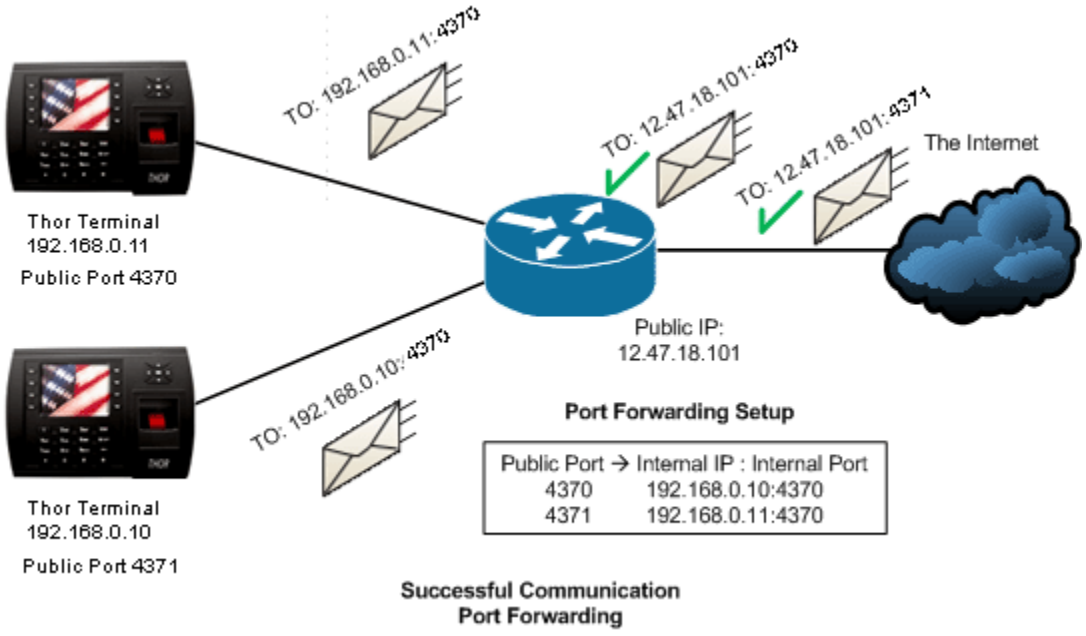
INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Port Forwarding - Port forwarding is a process that a router or firewall uses in order to direct the appropriate kind of network data to the correct internal device on a specific port. Returning to our Network : Town analogy, recall that a door is similar to a port. Why does one go through a door? To reach the room on the other side. Let's say that two visitors are arriving at your building for a company tour but they are not sure where to go. The first visitor is expecting a tour of the Office area while the second visitor is expecting a tour of the Production Facility. A receptionist would often perform the function of directing these visitors to the appropriate area in order to reach their destination. Port forwarding performs this same service. Traffic from the Internet arrives on a port at the public interface of the router or firewall. The router is configured to forward all traffic arriving on a specific port to a particular device on the inside of the network at a specific port. This is illustrated by the diagram below. The diagram illustrates traffic arriving from the Internet on two different ports. Port Forwarding configuration on the router specifies that all traffic inbound on port 4370 is to be delivered to the Internal IP Address of 192.168.0.10 at port 4370. Traffic inbound on port 4371 is delivered to the Internal IP Address of 192.168.0.11 at port 4370.



Successful Communication
Port Forwarding

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

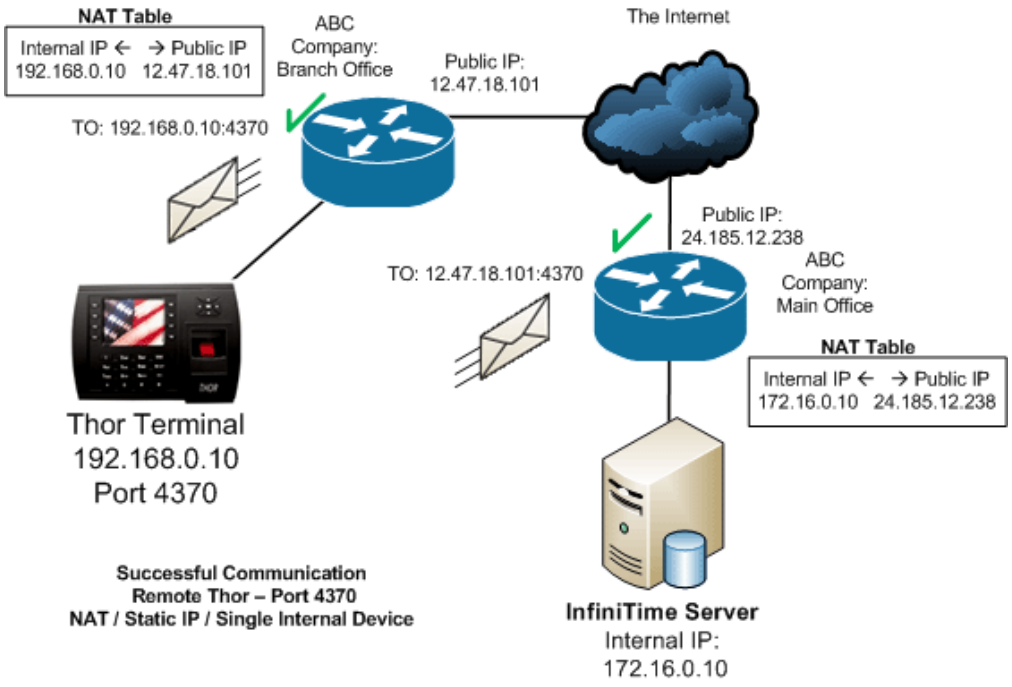
InfiniTime Labor Management Systems

Scenarios

Single Remote Site with a single Static Public IP Address // Single Internal Device

Some locations such as warehouses do not require Internet Access for day to day operations. In order to place an Ethernet Time and Attendance Data Collection Terminal such as the Thor or the Scout at such a location a connection to the Internet is required. Be sure to confirm with your chosen ISP that your public IP Address is static and write down the IP Address provided to you. This address will be required when configuring the InfiniTime Application to communicate with your remote device. It is important to note that a router is required to route packets and perform NAT services to and from your Time and Attendance terminal even though you will only have a single device on the network. Two methods are available to establish communication between the InfiniTime Server and an Ethernet Time and Attendance terminal located at a remote site with a single static IP Address and a single internal device. One option is to use NAT in order to forward all traffic sent to the Public IP Address directly to the clock. A second option is the use of port forwarding to send all traffic sent to a specific port on the Public IP Address to the clock. These methods are described below.

NAT - The diagram below illustrates the configuration of NAT for a remote site with a single Public IP Address where the Time and Attendance terminal will be the only item on the internal network.



INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

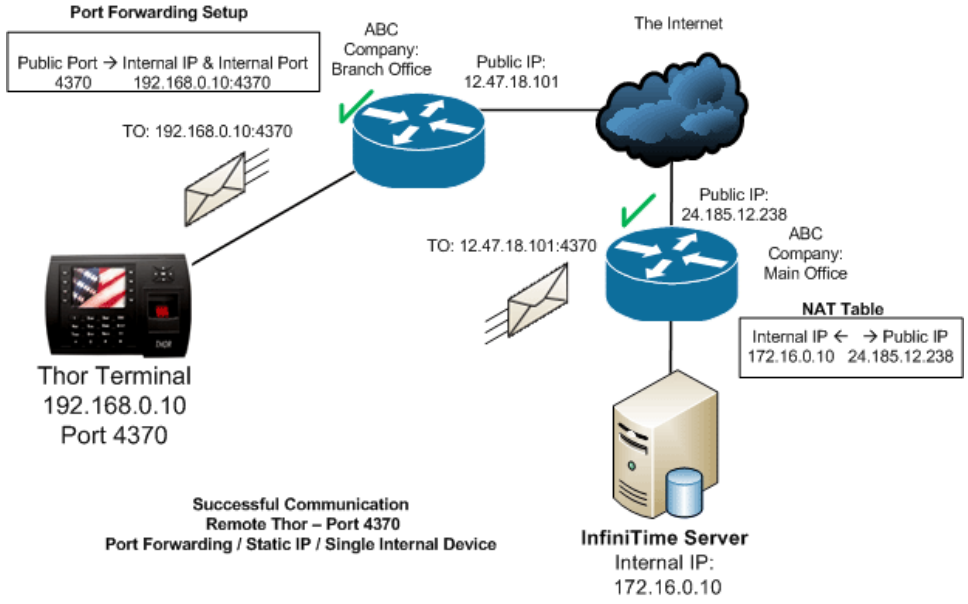
Information Technologies Brief

InfiniTime Labor Management Systems

Requirements - The following items are required in order for communication between the InfiniTime Server and the Thor Terminal to be successful. If you have difficulties communicating with your remote terminal verify each of the following items are configured correctly. You may also wish to refer to the troubleshooting guide below. The example does not accurately depict all possible network configurations. As a general rule any hardware or software firewall located between the source (The InfiniTime Server) and the destination (The Thor Terminal) must be configured to pass traffic on the chosen port and to trust the local network.

- Software Firewall on the InfiniTime Server must permit outbound traffic on port 4370
- Router at Main Office must permit inbound traffic on port 4370 on the Private Interface
- Router at Main Office must permit outbound traffic on port 4370 on the Public Interface
- ISP must pass traffic on port 4370. If you have difficulties with communication contact your ISP to verify the chosen port is open.
- Router at Branch Office must permit outbound traffic on port 4370 on the Private Interface
- Router at Branch Office must permit inbound traffic on port 4370 on the Public Interface
- Router at Branch Office must be configured appropriately for NAT with a static mapping between the Public IP Address and the Internal IP Address of the Ethernet terminal.
- Router at Branch Office must be configured to respond to PING as InfiniTime requires the ability to ping the destination IP Address.

Port Forwarding - The diagram below illustrates the configuration of Port Forwarding for a remote site with a single Public IP Address where the Time and Attendance terminal will be the only item on the internal network.



INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Requirements - The following items are required in order for communication between the InfiniTime Server and the Thor Terminal to be successful. If you have difficulties communicating with your remote terminal verify each of the following items are configured correctly. You may also wish to refer to the troubleshooting guide below. The example does not accurately depict all possible network configurations. As a general rule any hardware or software firewall located between the source (The InfiniTime Server) and the destination (The Thor Terminal) must be configured to pass traffic on the chosen port and to trust the local network.

- Software Firewall on the InfiniTime Server must permit outbound traffic on port 4370
- Router at Main Office must permit inbound traffic on port 4370 on the Private Interface
- Router at Main Office must permit outbound traffic on port 4370 on the Public Interface
- ISP must pass traffic on port 4370. If you have difficulties with communication contact your ISP to verify the chosen port is open.
- Router at Branch Office must permit outbound traffic on port 4370 on the Private Interface
- Router at Branch Office must permit inbound traffic on port 4370 on the Public Interface
- Port forwarding must be configured to send traffic to the default port as listed in the previous table for your Time and Attendance Terminal. It is not possible to change the listening port for these terminals.
- Router at Branch Office must be configured to respond to PING as InfiniTime requires the ability to ping the destination IP Address.

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

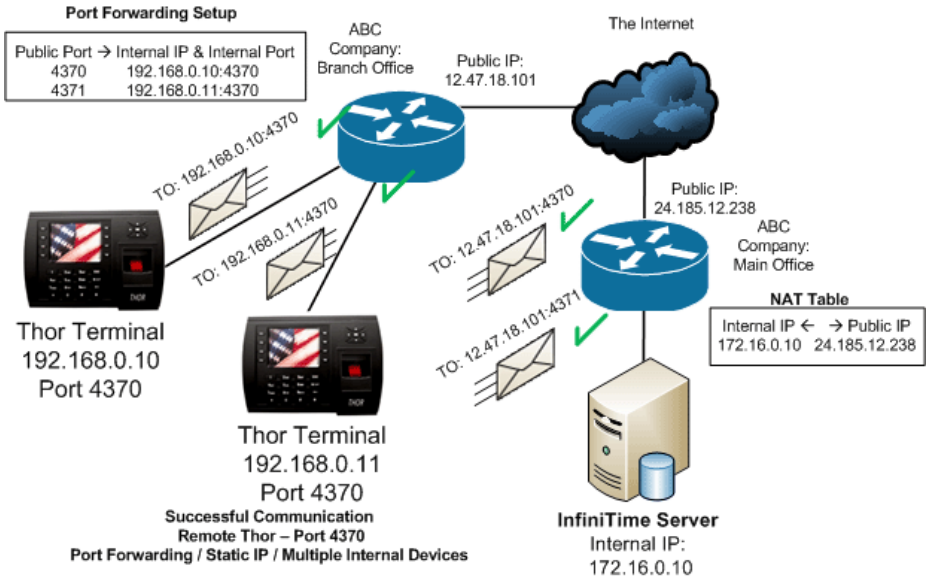
www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Single Remote Site with a single Static Public IP Address // Multiple Internal Devices

Port Forwarding - The diagram below illustrates the configuration of Port Forwarding for a remote site with a single Static Public IP Address where there are multiple devices on the internal network.



Requirements - The following items are required in order for communication between the InfiniTime Server and the Thor Terminal to be successful. If you have difficulties communicating with your remote terminal verify each of the following items are configured correctly. You may also wish to refer to the troubleshooting guide below. The example does not accurately depict all possible network configurations. As a general rule any hardware or software firewall located between the source (The InfiniTime Server) and the destination (The Thor Terminal) must be configured to pass traffic on the chosen port and to trust the local network.

- Software Firewall on the InfiniTime Server must permit outbound traffic on ports 4370 and 4371.
- Router at Main Office must permit inbound traffic on ports 4370 and 4371 on the Private Interface
- Router at Main Office must permit outbound traffic on ports 4370 and 4371 on the Public Interface
- ISP must pass traffic on ports 4370 and 4371 . If you have difficulties with communication contact your ISP to verify the chosen port is open.
- Router at Branch Office must permit outbound traffic on ports 4370 and 4371 on the Private Interface
- Router at Branch Office must permit inbound traffic on ports 4370 and 4371 on the Public Interface
- Port forwarding must be configured to send traffic to the default port as listed in the previous table for your Time and Attendance Terminal. It is not possible to change the listening port for these terminals. As shown in the diagram traffic from multiple public ports can be directed to the default port for separate Internal IP Addresses.

Information Technologies Brief

InfiniTime Labor Management Systems

- Router at Branch Office must be configured to respond to PING as InfiniTime requires the ability to ping the destination IP Address.

Single Remote Site with multiple Static Public IP Addresses // Multiple Internal Devices

Choose a single Public IP Address for use with your remote Ethernet Time and Attendance Terminals and follow the instructions above for a Single Remote Site with a single Static Public IP Address // Multiple Internal Devices.

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

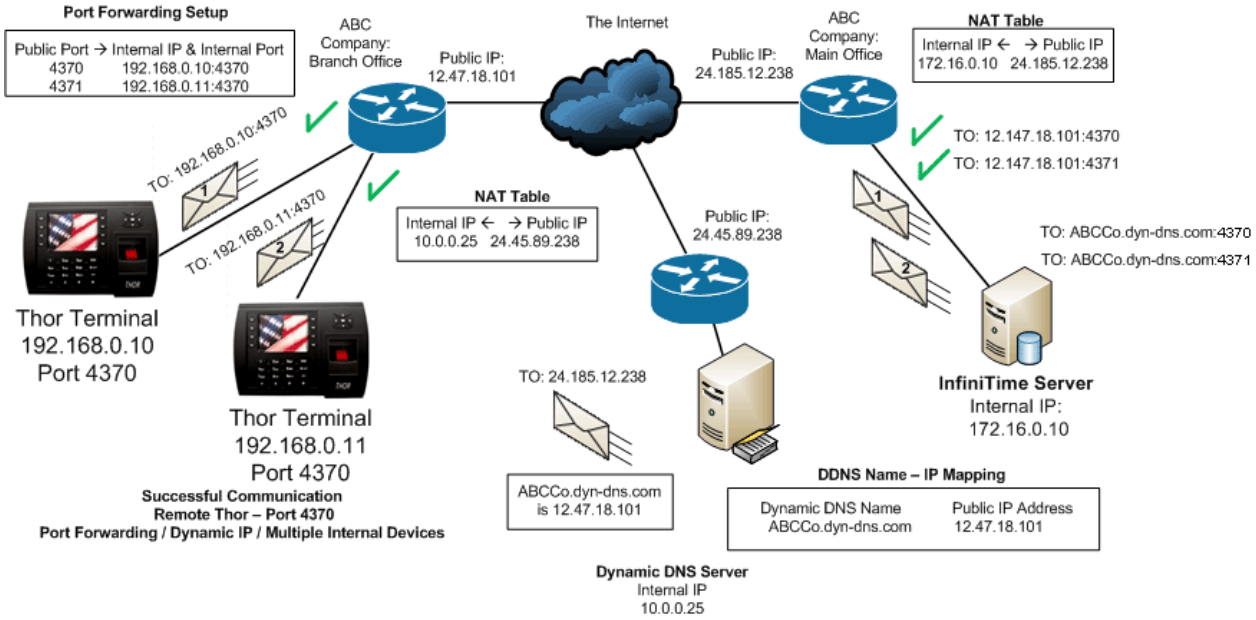
Information Technologies Brief

InfiniTime Labor Management Systems

Single Remote Site with a single Dynamic Public IP Address // Multiple Internal Devices

In some cases it is not possible to obtain a Static Public IP Address. This is often the case when using a non-commercial Internet Service such as residential DSL or Cable as many Internet Service Providers (ISP) will not provide a Static Public IP Address for these connection types. If a Static Public IP Address is not available Dynamic DNS (DDNS) must be used to map your Public IP Address to a DDNS domain. The DDNS service will map the DDNS domain name to your Public IP Address and will change the mapping as your Public IP Address changes.

Dynamic DNS w/ Port Forwarding - The diagram below illustrates the configuration of Dynamic DNS with Port Forwarding for a remote site with a single Public IP Address where there are multiple devices on the internal network.



Traffic Flow

Infinitime Server wishes to send data to ABCCO.dyn-dns.com at port 4370 and 4371. Remember, computers do not understand words or phrases and must translate the DDNS Name "ABCCo.dyn-dns.com" to an IP Address. Once an IP Address has been associated with the domain name communication continues as normal.

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Requirements - The following items are required in order for communication between the InfiniTime Server and the Thor Terminals to be successful. If you have difficulties communicating with your remote terminals verify each of the following items are configured correctly. You may also wish to refer to the troubleshooting guide below. The example does not accurately depict all possible network configurations. As a general rule any hardware or software firewall located between the source (The InfiniTime Server) and the destination (The Thor Terminal) must be configured to pass traffic on the chosen port and to trust the local network.

- Software Firewall on the InfiniTime Server must permit outbound traffic on ports 4370 and 4371
- Router at Main Office must permit inbound traffic on ports 4370 and 4371 on the Private Interface
- Router at Main Office must permit outbound traffic on ports 4370 and 4371 on the Public Interface
- ISP must pass traffic on ports 4370 and 4371. If you have difficulties with communication contact your ISP to verify the chosen port is open.
- Router at Branch Office must permit outbound traffic on ports 4370 and 4371 on the Private Interface
- Router at Branch Office must permit inbound traffic on ports 4370 and 4371 on the Public Interface
- Dynamic DNS must be configured appropriately to route traffic to your network.
- Port forwarding must be configured to send traffic to the default port as listed in the previous table for your Time and Attendance Terminal. It is not possible to change the listening port for these terminals. As shown in the diagram traffic from multiple public ports can be directed to the default port for separate Internal IP Addresses.
- Router at Branch Office must be configured to respond to PING as InfiniTime requires the ability to ping the destination IP Address.

Single Remote Site with a single Dynamic Public IP Address // Single Internal Device

In some cases it is not possible to obtain a Static Public IP Address. This is often the case when using a non-commercial Internet Service such as residential DSL or Cable as many Internet Service Providers (ISP) will not provide a Static Public IP Address for these connection types. If a Static Public IP Address is not available Dynamic DNS (DDNS) must be used to map your Public IP Address to a DDNS domain. The DDNS service will map the DDNS domain name to your Public IP Address and will change the mapping as your Public IP Address changes.

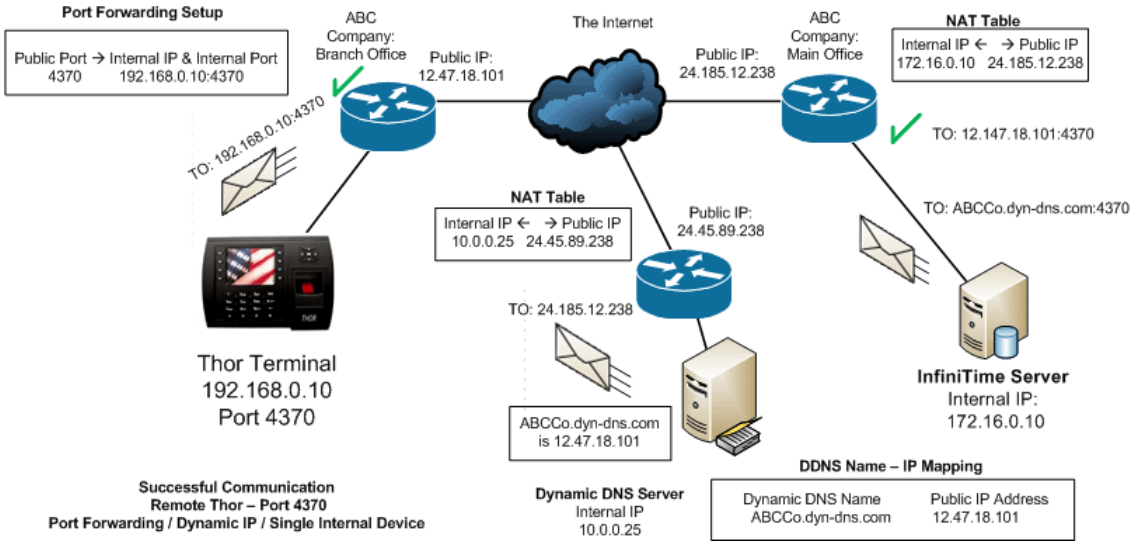
INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Dynamic DNS w/ Port Forwarding - The diagram below illustrates the configuration of Dynamic DNS with Port Forwarding for a remote site with a single Public IP Address where the Time and Attendance terminal will be the only item on the internal network.



Traffic Flow

Infinitime Server wishes to send data to ABCCO.dyn-dns.com at port 4370. Remember, computers do not understand words or phrases and must translate the DDNS Name "ABCCo.dyn-dns.com" to an IP Address. Once an IP Address has been associated with the domain name communication continues as normal.

Requirements - The following items are required in order for communication between the InfiniTime Server and the Thor Terminals to be successful. If you have difficulties communicating with your remote terminals verify each of the following items are configured correctly. You may also wish to refer to the troubleshooting guide below. The example does not accurately depict all possible network configurations. As a general rule any hardware or software firewall located between the source (The InfiniTime Server) and the destination (The Thor Terminal) must be configured to pass traffic on the chosen port and to trust the local network.

- Software Firewall on the InfiniTime Server must permit outbound traffic on port 4370
- Router at Main Office must permit inbound traffic on port 4370 on the Private Interface
- Router at Main Office must permit outbound traffic on port 4370 on the Public Interface
- ISP must pass traffic on port 4370. If you have difficulties with communication contact your ISP to verify the chosen port is open.
- Router at Branch Office must permit outbound traffic on port 4370 on the Private Interface

Information Technologies Brief

InfiniTime Labor Management Systems

- Router at Branch Office must permit inbound traffic on port 4370 on the Public Interface
- Dynamic DNS must be configured appropriately to route traffic to your network.
- Port forwarding must be configured to send traffic to the default port as listed in the previous table for your Time and Attendance Terminal. It is not possible to change the listening port for these terminals. As shown in the diagram traffic from multiple public ports can be directed to the default port for separate Internal IP Addresses.
- Router at Branch Office must be configured to respond to PING as InfiniTime requires the ability to ping the destination IP Address.

Single Remote Site with multiple Dynamic Public IP Addresses // Multiple Internal Devices

Choose a single Public IP Address for use with your remote Ethernet Time and Attendance Terminals and follow the instructions above for a Single Remote Site with a single Static Public IP Address // Multiple Internal Devices.

INCEPTION TECHNOLOGIES
TIME & ATTENDANCE SOLUTIONS
6097 North 57th Drive · Glendale, Arizona 85301

www.InfiniTime.com
Support@InceptionTechnologies.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Information Technologies Brief

InfiniTime Labor Management Systems

Troubleshooting

Even though there are multiple points of failure a standard troubleshooting procedure can be used to quickly identify most issues. If you should experience difficulties or receive excessive errors when attempting to communicate with your remote Ethernet Terminal from within the InfiniTime Application follow the steps below to locate the source of the problem.

1.) Ping the Static IP Address assigned to the Time and Attendance Terminal from another computer on the remote network. If the Ethernet terminal should fail to respond verify the items below. Additional instructions for configuring these items can be found in the Hardware Manual for your specific terminal.

- Verify your Ethernet Terminal is plugged in.
- Check for issues related to the Ethernet cable.
  - Replace the cable if any cuts or slices are evident in the cable run.
  - Fix the cable if the cable ends are improperly terminated.
  - Test the cable with a laptop to verify the cable is properly wired, or use a wire tester if available.
  - Verify the cable is connected to the correct port on your Ethernet terminal.
  - Try using a different port on your hub, switch, or router.
  - The Ethernet Cable run should not exceed 100 meters. (328 ft.)
- Verify Network Information is correct
  - The Ethernet Terminal must be assigned a static IP address. Contact your network administrator if you are unsure if the address you have is static.
  - Default Gateway
  - Subnet Mask

- Check Ethernet Terminal Configuration
  - Ethernet Terminal IP Address
  - Ethernet Terminal Subnet
  - Default Gateway
  - Peer Address should be set to 000.000.000.000*
  - Host Bits*

*Only applies to specific Time and Attendance Hardware Models.

- Check Software Configuration
  - IP address
  - Port
  - Reader Address

Information Technologies Brief

InfiniTime Labor Management Systems

2.) Ping the Public IP Address of the remote router. If the router should fail to reply verify the items below.

- The router must be configured to respond to PING.
- Verify the Internet Connection at the main and remote site(s) is up.

3.) If communication errors should still occur after verifying the aforementioned items there is most likely an issue with NAT or Port Forwarding. It is also possible that traffic is being blocked before it gets to the destination. Verify all hardware or software firewalls between the source and destination are configured to permit traffic on the chosen ports. It may also help to check with your ISP to see if they are blocking traffic on any ports.