



by Honeywell

IP Communicator Site Checklist

Operation:

The IP COMMUNICATOR captures the contact-ID signals dialed out the panel telephone dialer ports and converts them into Ethernet packets. These packets are sent out the customer's shared network equipment to the Internet and are received at a special Central Station receiver where they are converted back into contact-ID signals as if they were received over a telephone line. Therefore, the panel will be programmed as if it were connecting to two telephone lines and an Ethernet connection to the Internet must be provided by the customer.

The IP Communicator will require minimal programming with some information obtained from the customer's IT personnel and other information obtained from the central station. Larger sites such as corporate networks typically require the involvement of an IT director. The document provided on the next 2 pages is designed to be printed and provided to the customers IT director. It outlines requirements and provides a detailed explanation of the bandwidth requirements and minimal volume of data that will be placed on the network.

If the site does not have IT personnel, you will need to determine how the customer connects computer equipment to the Internet. If the customer uses a DSL modem or Cable modem, the operation will typically assign an IP address to the IP Communicator automatically using DHCP protocol. In this case you will only need to program the IP Communicator for DHCP and ignore any settings for static IP address. (See programming instructions.)

If a corporation is involved and a private network is established with or without static IP addresses with specific established network policies, you will be required to gather the following information from the IT director to use when programming the IP Communicator.

IP Communicator Site Checklist			
Customer Name			
<input type="checkbox"/> Dynamic IP Address will be used (DHCP is available)			
<input type="checkbox"/> Static IP Address will be used			
If Static Address is Used			
IP Communicator IP Address		Subnet Mask	
Router / Switch IP Address			
Information Required From Central Station			
Account Number		UDP Port #	
Primary Receiver IP Address		Installer Password	
Secondary Receiver IP Address			



by Honeywell

IP Communicator Site Checklist

Overview for IT Directors:

System IP traffic flows

All the IP traffic exchanged between the IP Communicator network appliance and the Central Station VisorALARM receiver utilizes UDP protocol over the Internet. This traffic runs on a single UDP connection (i.e. a single UDP port). Although the UDP frame payload is encrypted, the frame header is sent without any encryption, so all network equipment can process and forward them without any restriction at all, just as they do with any other application traffic based on UDP (IP telephony audio streams, video streams, etc).

As such, the UDP header of all frames transmitted from the IP Communicator to the VisorALARM:

- Have both the UDP source and destination ports set to the VisorALARM serving port value (UDP port 80, by default). This port is manually configured by the installer.
- Have the source IP address set to the IP Communicator local IP address. This address is manually configured as static or obtained from DHCP.
- Have the destination IP address set to the VisorALARM IP translated address. This IP address is also manually configured in the IP Communicator during installation.
- All UDP frames are transmitted through the IP Communicator default gateway IP address.

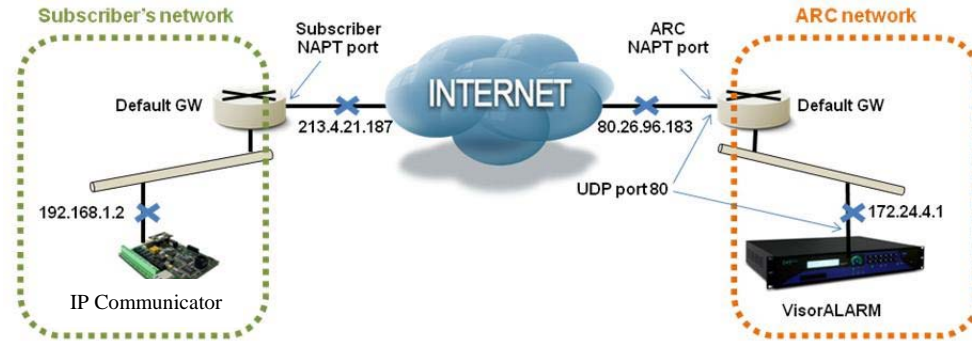
In analogy, all UDP frames sent back from the VisorALARM to the IP COMMUNICATOR:

- Have the UDP source port value set to the VisorALARM serving port (UDP port 80, by default).
- Have the destination UDP port set to the IP COMMUNICATOR port, which was learned by the VisorALARM from the last IP Communicator keep-alive frame received.
- Have the source IP address set to the VisorALARM LAN port IP address.
- Have the destination IP address set to the IP Communicator address, which was learned in the VisorALARM from the last keep-alive received.
- Are transmitted through the VisorALARM default gateway IP address.

In a typical scenario, the IP Communicator and VisorALARM default gateways are connected to the Internet. The UDP frames transmitted to the Internet through these gateways are hence modified according to NAT, (Network Address Port Translation).

The following diagram illustrates a network diagram for this scenario as well as the UDP frame header parameters in each network segment (subscriber network, the Internet and the Alarm Receiving Central network (ARC):

IP Communicator Site Checklist



		UDP frame header parameters			
Transmission flow	Network	Source IP address	Destination IP address	Source Port	Destination port
IPDACT → VisorALARM	Subscriber	192.168.1.2	80.26.96.183	80	80
	Internet	213.4.21.187	80.26.96.183	Subscriber NAPT port	80
	ARC	213.4.21.187	172.24.4.1	Subscriber NAPT port	80
VisorALARM ← IPDACT	ARC	172.24.4.1	213.4.21.187	80	Subscriber NAPT port
	Internet	80.26.96.183	213.4.21.187	ARC NAPT port	Subscriber NAPT port
	Subscriber	80.26.96.183	192.168.1.2	ARC NAPT port	80

Figure 1. NAPT scenario and UDP frame header conversions

Note that if the subscriber's network has a DHCP server operating, the unit can be configured to not require a static IP address. However, if IT policies so dictate, a static IP address/mask can be added during installation along with the default gateway address.

As we can observe in Figure 1, both routers need to do NAPT so the transmitted UDP frame travels along the Internet with the system public IP addresses (213.4.21.187 and 80.26.96.183 in the Figure). For the correct system operation, the subscriber's network firewall should allow:

- ❑ UDP traffic sent from the IP Communicator (IP address: 192.168.1.2 in the example) to the ARC public IP address (80.26.96.183 in the example). On transmission, the subscriber's default gateway sets a NAPT conversion entry in its cache memory, so the received UDP traffic from the Internet can be forwarded back to the IP Communicator.
- ❑ UDP traffic received from the ARC (80.26.96.183). The subscriber's default gateway will forward this traffic to the IP Communicator (192.168.1.2) according to its cached NAPT entry.

In analogy, the ARC network firewall should allow:

- ❑ UDP traffic received from the Internet to its serving port (port 80 in the example). Traffic to this port should be triggered to the VisorALARM (IP address: 172.24.4.1, serving port 80).
- ❑ UDP traffic sent from the VisorALARM to the Internet.

It is required that all network appliances between the fire panel and actual Internet gateway be battery backed by a UPS for a minimum of 4 hours.