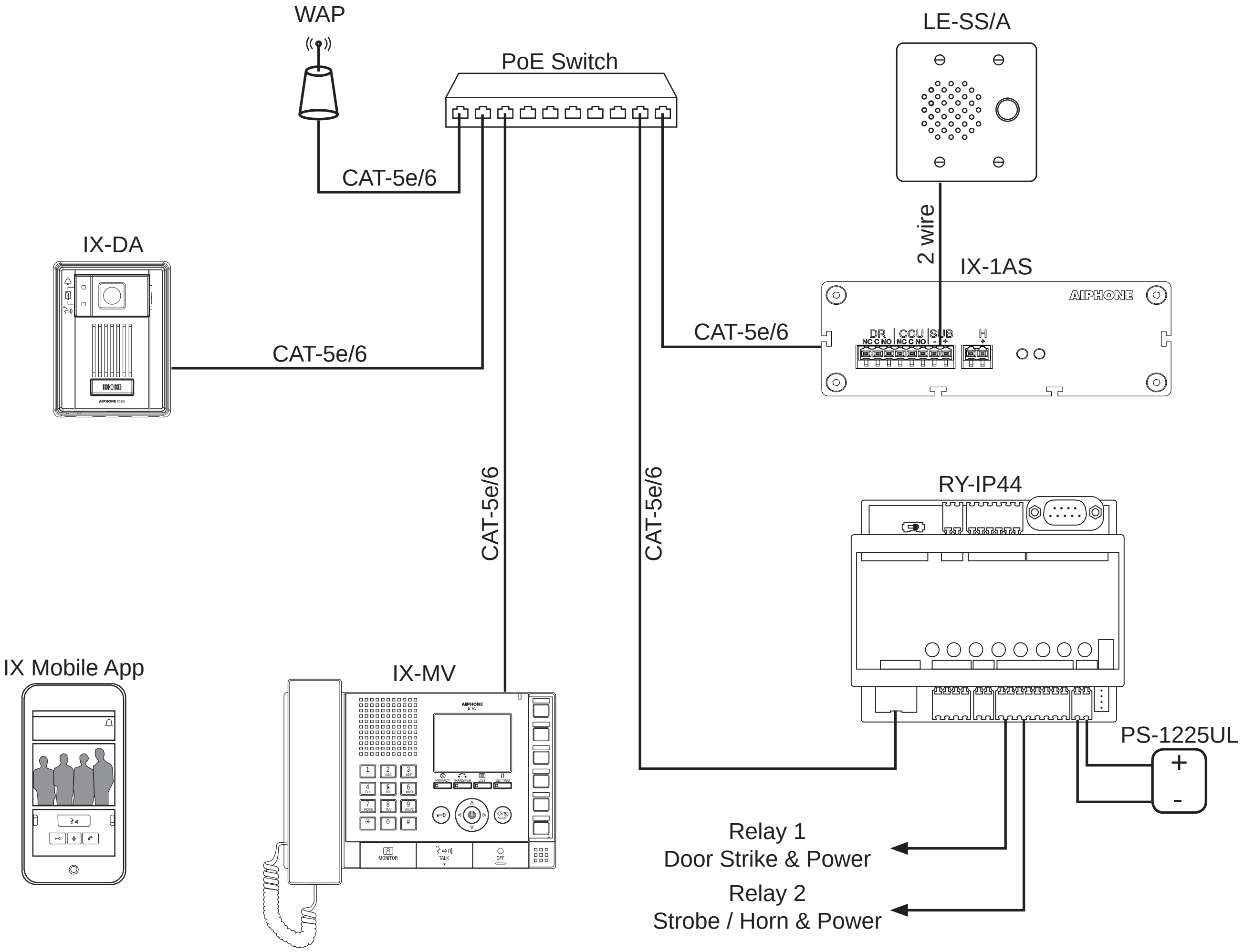
IX Series Protocol

The IX Series has a variety of IP video door stations, IP audio only door stations, and 2-wire adaptors for legacy intercoms. Calls may be answered and doors may be unlocked by IX-MV master stations and the IX Mobile app.

The RY-IP44 relay allows the IX Mobile app to detect when the mobile device is within range of the network to receive calls, and to notify the user when the mobile device has left the network.

The IX Support Tool is used to configure and make changes to an IX Series system.

Wiring



Protocol Overview

IX-DA, IX-BA
Door Stations

- IPv4 or IPv6
- “Peer to Peer” SIP for signaling, RTP and RTCP for audio and video
- If enabled, will use DHCP, IGMP / MLD for multicast, NTP, SMTP and DNS as needed
- If enabled, uses SIF, CGI for integration (these might use SSL/TLS, depending on configuration)
- Configuration is through web (HTTPS) or through IX Support Tool (SSH)

IX-MV Master Station

- IPv4 or IPv6
- “Peer to Peer” SIP for signaling, RTP and RTCP for audio and video
- If enabled, will use DHCP, IGMP / MLD for multicast, NTP, SMTP and DNS as needed
- If enabled, uses SIF, CGI for integration (these might use SSL/TLS, depending on configuration)
- Configuration is through web (HTTPS) or through IX Support Tool (SSH)

RY-IP44 I/O Relay
Adaptor & App Server

- IPv4 only
- Reads SIF messages and issues CGI commands
- If enabled, will use DHCP
- Does not use SSL/TLS, nor SSH
- Configuration is through web only (HTTP)

IX-1AS / IX-10AS
2-Wire Station Adaptor

- IPv4 only
- Sends SIF messages
- “Peer to Peer” SIP for signaling, RTP for audio
- DHCP by default (can set static)
- Does not use SSL/TLS, nor SSH
- Configuration is through web only (HTTP)

IX Mobile App

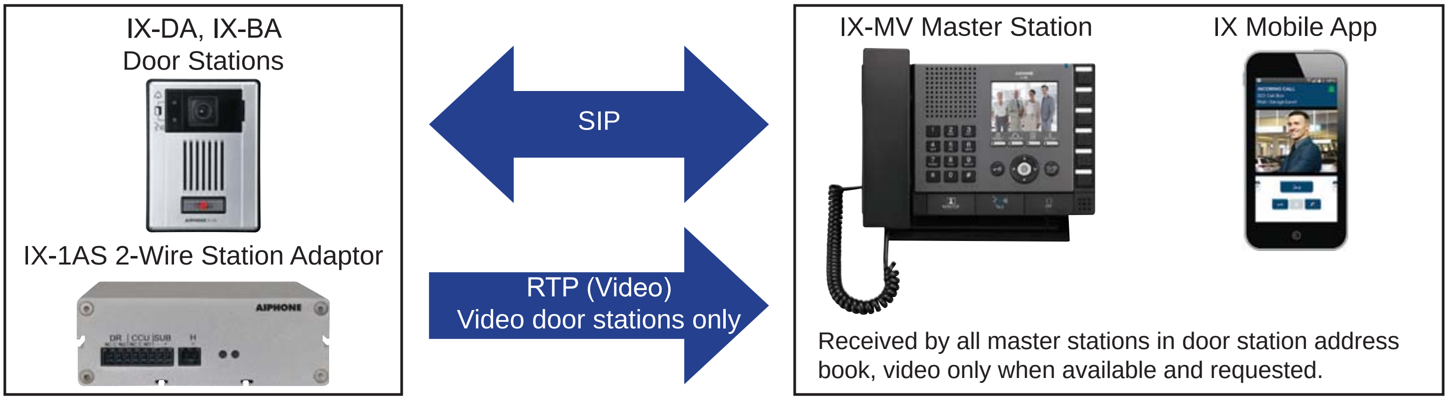
- IPv4 only
- “Peer to Peer” SIP for signaling, RTP and RTCP for audio and video
- If enabled, will use DHCP, IGMP / MLD for multicast, NTP, SMTP and DNS as needed
- If enabled, uses SIF (SIF might use SSL/TLS, depending on configuration)
- Configuration file can be transferred through iTunes® (iOS only), USB, or other methods (Android™ only)

Ports and Protocols

Protocol	**Overview**		**Notes**
IPv4	All IX Series stations		
IPv6	All IX Series stations (**except noted)*		*IX Mobile, IX-1AS/10AS, RY-IP44
TCP	SIF, CGI		
UDP	SIP, IX Series Paging		
ICMP	Internet control message protocol		
ARP	Address resolution protocol		
Protocol	**Default Value**	**Can change?**	**Notes**
SIP	5060	Yes	Uses IX Series headers, which makes it proprietary
HTTP	80	No	Accepts CGI commands described in SIF/CGI protocol docs
HTTPS	443	No	Web configuration interface + HTTPS CGI commands
RTSP	10080	No	For when ONVIF communication does not work
RTP	20000 - 30000 ranges	Yes	Audio and Video
RTCP	20000 - 30000 ranges	Yes	
IGMP	-	-	Join and leave requests based on SDP information
MLD	-	-	Join and leave requests based on SDP information
SMTP	25	Yes	Email feature (requires DNS)
FTP over SSH	8715 and 22	No	Used by IX Support Tool to update configurations
DHCP	68	No	DHCP client
NTP	123	Yes	Network time
DNS	53	No	DNS for email domain name lookup
IX Paging	55550	No	IX Series paging control messages
IX Paging	55552 and up	No	IX Series Paging Audio
IX SIF	10000	Yes	Sends SIF messages as described in SIF/CGI protocol docs
IX Door Release	8620	No	Door release
App Server	5061	Yes	Apps communicate with App Server for presence detection
IX Search and Associate	8700	No	UDP all subnets broadcast, only MAC address in message reacts to associate, all respond to search

Call Flow Diagrams

Call Started



IX-DA, IX-BA Door Stations

IX-1AS 2-Wire Station Adaptor

SIP

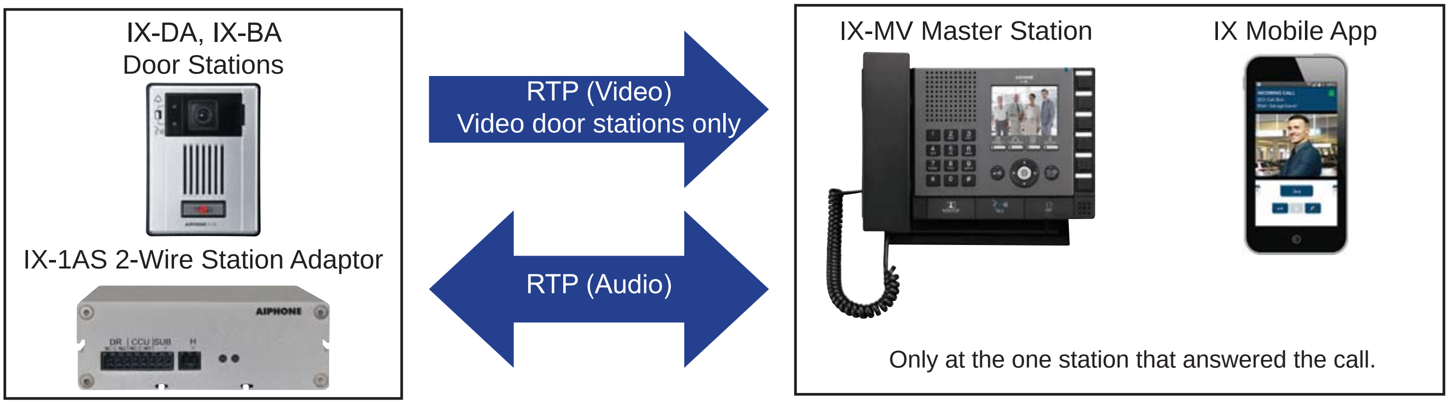
RTP (Video) Video door stations only

IX-MV Master Station

IX Mobile App

Received by all master stations in door station address book, video only when available and requested.

Call Answered



IX-DA, IX-BA Door Stations

IX-1AS 2-Wire Station Adaptor

RTP (Video) Video door stations only

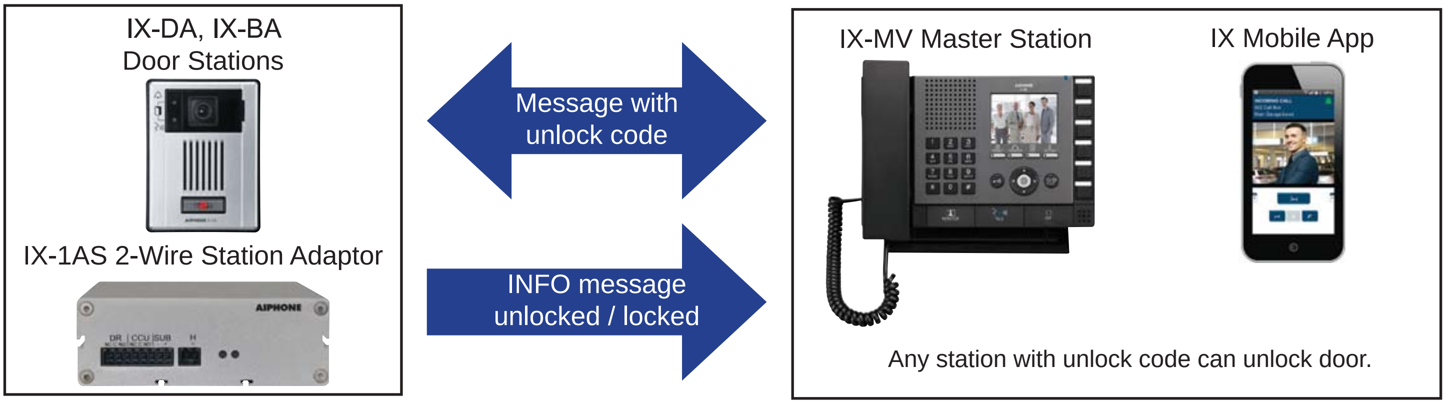
RTP (Audio)

IX-MV Master Station

IX Mobile App

Only at the one station that answered the call.

Door Release



IX-DA, IX-BA Door Stations

IX-1AS 2-Wire Station Adaptor

Message with unlock code

INFO message unlocked / locked

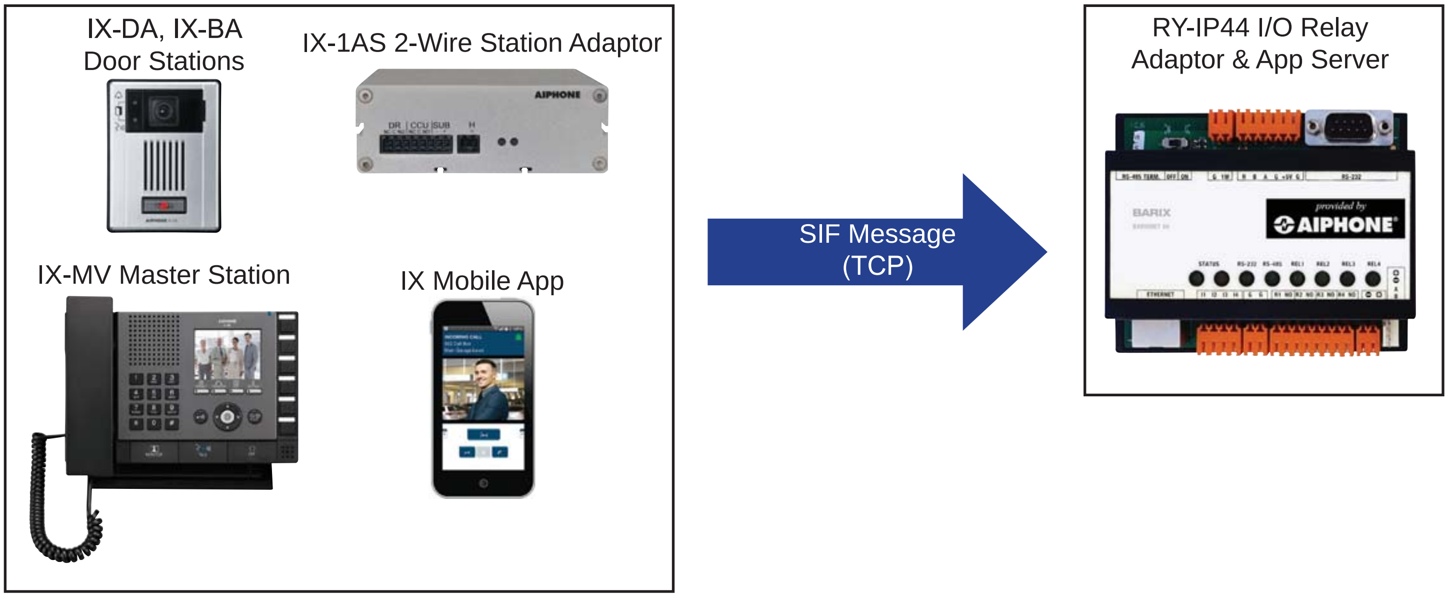
IX-MV Master Station

IX Mobile App

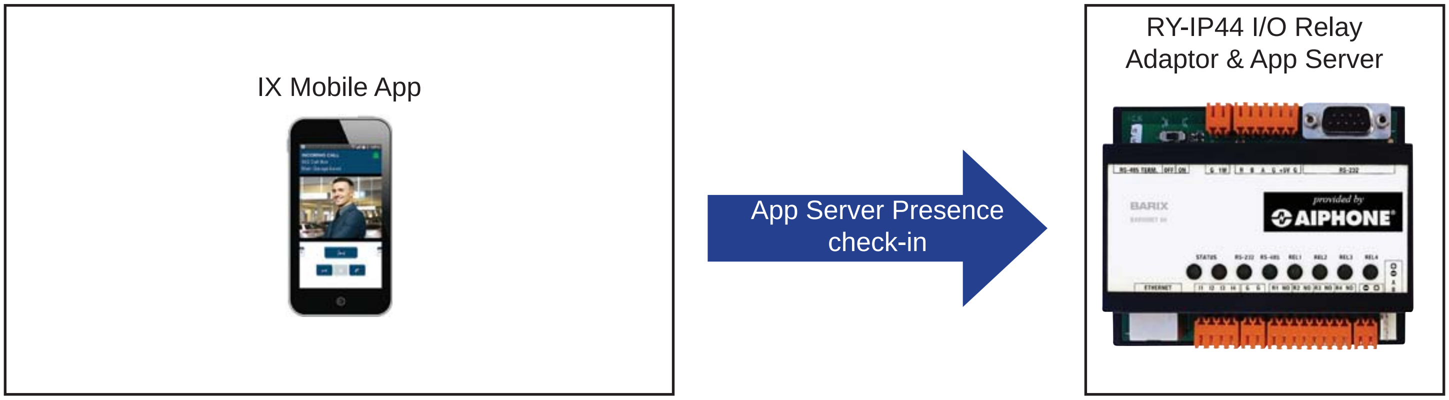
Any station with unlock code can unlock door.

Call Flow Diagrams *(cont.)*

SIF Events

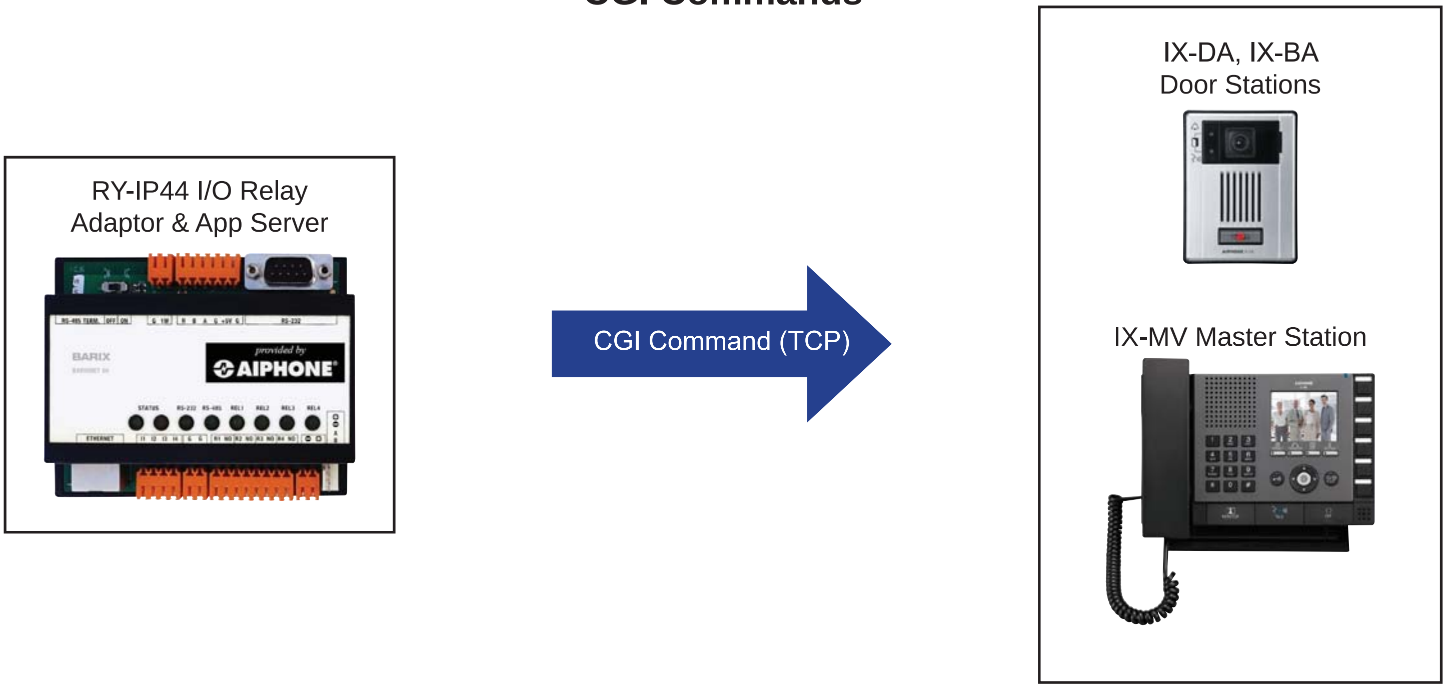


App Server Check-in



Call Flow Diagrams *(cont.)*

CGI Commands



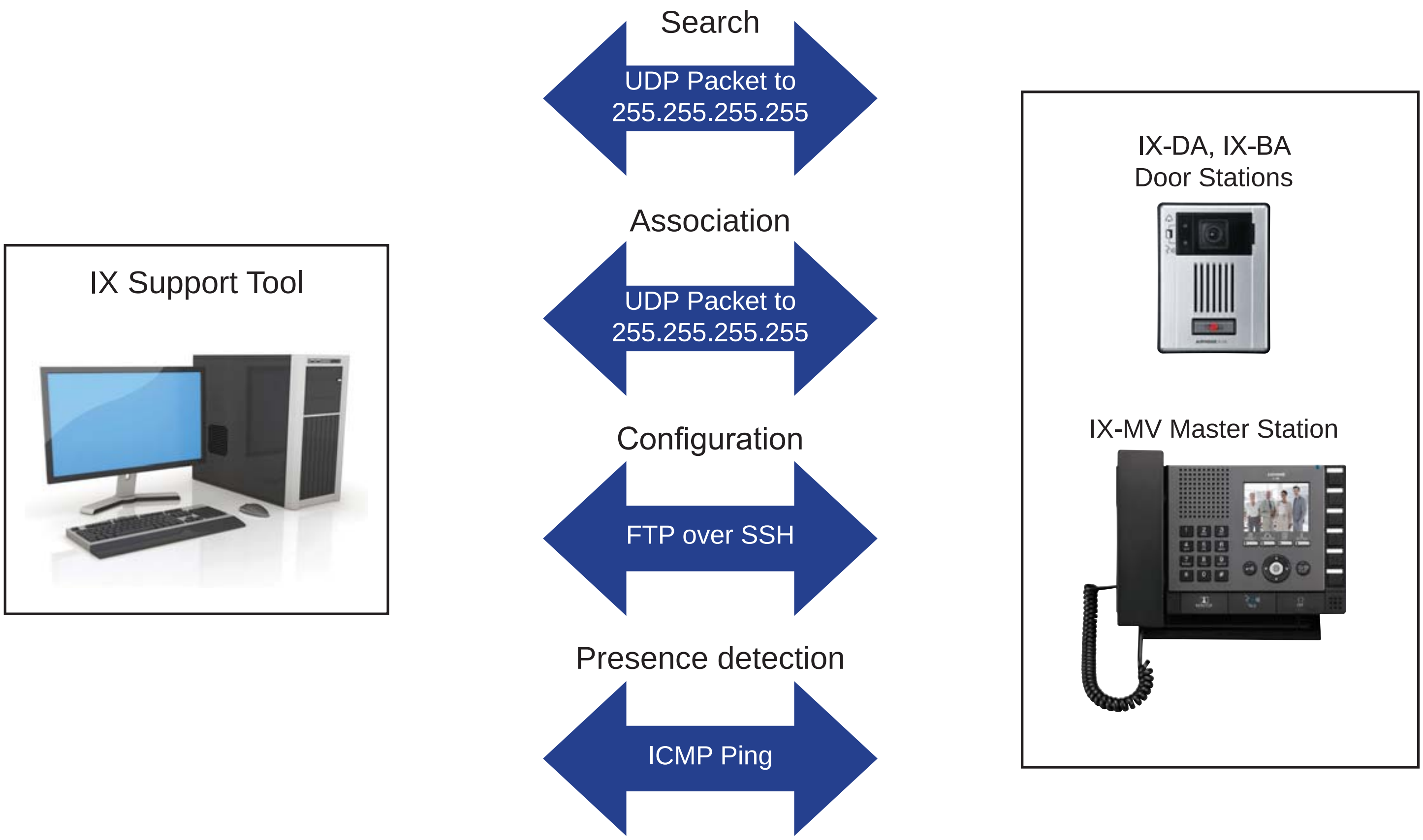
RY-IP44 I/O Relay Adaptor & App Server

CGI Command (TCP)

IX-DA, IX-BA Door Stations

IX-MV Master Station

IX Support Tool Functions



IX Support Tool

Search

UDP Packet to 255.255.255.255

Association

UDP Packet to 255.255.255.255

Configuration

FTP over SSH

Presence detection

ICMP Ping

IX-DA, IX-BA Door Stations

IX-MV Master Station

Best Practices

Using the IX Support Tool

Each intercom can have its own Admin ID and password as well as a User ID and password. These are typically managed via the IX Support Tool, but can be changed in the web interface. The IX Support Tool itself has its own ID and password.

The IX Support Tool generates files that are sensitive from a security standpoint. The IX Support Tool should be located on a PC that normal users will not access. While these files are transported safely to their intended destinations, the storage of these files is not secure. Just like a normal user is not going to have physical access to the file server, a normal user should not have physical access to the PC running the IX Support Tool.

IX Mobile relies on having an accurate configuration file generated by the IX Support Tool. If a user wants the configuration file, the best way to deliver it is through a secure method, such as putting the configuration file on a secured FTP server or a secure file server. These files contain specific passwords stored in plain text. An experienced user could read this configuration file and discover the admin password for the intercom (the mobile app, not other intercom stations). They would also be able to discover the door release codes used to authorize access to certain doors. Consider protecting mobile devices with encryption, pin codes, and remote wipe capabilities.

Using a Browser

When using a browser to make changes, be aware of the possibility of a Man in the Middle (MitM) attack if the browser makes a connection using anything other than TLS 1.2. The IX Series stations will accept incoming legacy SSL 3.0, TLS 1.0, and TLS 1.1 connections, however these are not secure against MitM attacks. Never enter your admin ID and password using a browser connected with these protocols.

Do not modify the configuration of the RY-IP44 nor IX-1AS / IX-10AS adaptors outside of the LAN. Inside a LAN, passwords protect the configuration from local users. These devices do not use SSL or TLS, nor do they accept SSH configurations from the IX Support Tool. Ensure no one except the administrator will have access to the web configuration port (port 80). This is typically done using access control lists, isolated VLANs, or similar security measures.

Outside a LAN, the best way to modify an IX Series system is to remotely access the PC running the IX Support Tool, then launch the IX Support Tool and make changes. Use a Remote Access system the administrator feels is secure. Launch a web browser on the remotely controlled PC running the IX Support Tool to change the configuration for RY-IP44 or IX-1AS / IX-10AS adaptors.