

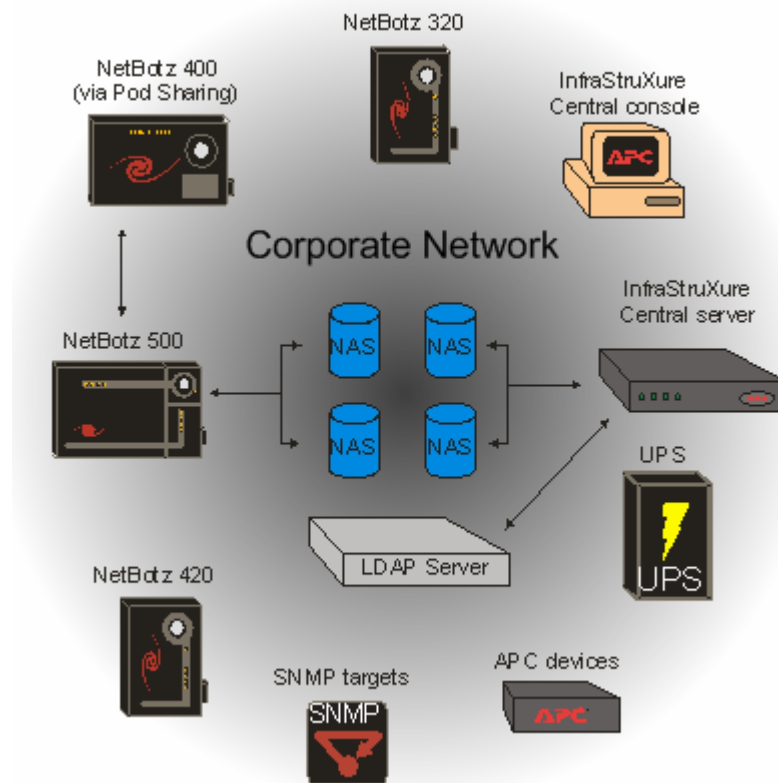
## How InfraStruXure® Central Server v5.x Relates to Your Network

### Introduction

This Application Note explains how InfraStruXure Central Server v5.x relates to your network, provides information on the discovery process, and other network-based functionality, and how the operations relate to your network.

### Corporate Network

InfraStruXure Central is a server appliance, which is accessed remotely from client workstations through the InfraStruXure Central console. The InfraStruXure Central console is a Java application that can be installed on a Windows or Linux workstation. InfraStruXure Central enables centralized management of APC devices, NetBotz appliances, and supported multi-vendor devices.



## Discovery

### Device licenses

The maximum number of supported devices that an individual InfraStruXure Central can discover and manage is dependent upon the device license installed. Should you attempt to add devices that exceed the license limit, InfraStruXure Central will notify you that the maximum number of available manageable devices has been exceeded and will not permit you to discover additional new devices. However you can choose which devices to monitor by removing non-essential devices and adding more critical ones. License packs that enable you to manage 25, 100, 500, or 1000 additional devices are available for purchase separately, and can be added at any time.

InfraStruXure Central has a limit on the maximum number of device licenses that can be added. **Table 1** shows the device license limitations for each platform.

**Table 1 – Device license limitations**

Platform	Device License Limit
Basic	525
Standard	2025
Enterprise	4025

However, certain practical limits – such as available network bandwidth, the amount of camera-related activity that occurs, and the manner in which your network administrators will use the InfraStruXure Central console – should certainly be taken into account when determining how many licensed devices will be monitored and managed by each InfraStruXure Central server. For example, if you'll be deploying APC NetBotz appliances strictly for the purposes of gathering environmental data and generating alerts, then a single InfraStruXure Central server could conceivably monitor and manage thousands of APC NetBotz appliances. On the other hand, if you're going to interactively manage and monitor the clients (such as planning to use the Surveillance view as an interactive display), then the interface itself will limit the number of clients that can reasonably be managed.

### Device discovery

InfraStruXure Central can discover supported devices on your network. Using the "Edit -> Add Devices" option, you can specify an IP address range that will be scanned on your network for the presence of supported devices. Scans can be user-initiated or can be performed automatically according to a user-specified schedule. Once this information is provided, InfraStruXure Central performs an SNMP or HTTP query to each IP address in the specified range.

If an APC device is not using the IP address to which the query was sent, InfraStruXure Central will not receive its requested data and will then move onto the next IP address in the range. This process will repeat until all IP addresses in the range have been checked. If a device is discovered, information about the device (type and model, for instance, as well as sensor information) is obtained and the device is then added to the device list within InfraStruXure Central.

## Network traffic

InfraStruXure Central network utilization is highly dependant on how your supported devices are configured and how much data is collected from the supported devices. As previously noted, during the initial discovery process, network communications are minimal and should result in no noticeable impact on network performance (no more than approximately 100 bytes per IP address in the specified discovery IP range). However, if a NetBotz device with a large amount of sensor history or alert data is discovered, the process of retrieving all of the stored data can result in a one-time only use of a significant amount of network bandwidth.

For example, if InfraStruXure Central discovers an APC NetBotz 500 that has 24 hours worth of environmental monitoring data and some alerts that include camera images stored in its integrated memory this might result in 2-3 MB of data being transferred across the network. On the other hand, if this same APC NetBotz 500 is using an external storage system to store 6 months of environmental data and alerts, including large amounts of video images, then a one-time transfer of several gigabytes of data from the appliance to the server is not unusual. Note that this data transfer occurs only once, upon initial discovery of the appliance. Once the data has been retrieved, network utilization should return to normal levels (approximately 100-200kb of updated sensor data once every 15 minutes, by default, and alert data only when alerts actually occur).

Once the discovery process is complete, the manner in which the individual devices are deployed and configured to send data to the InfraStruXure Central server becomes far more significant. If devices are configured to send only numeric and static sensor data, and video and audio data are kept to a minimum, then the impact on network usage is negligible. However, if your appliances frequently generate large amounts of audio/video data then, depending on network speed and topology, the impact on network resources could be significant.

## Appliance camera settings and network traffic

**Table 2** shows the approximate size of the image files generated by the NetBotz appliance camera at each of the supported resolutions as well as the maximum number of images that can be captured and generated each second. You can use this chart to estimate and plan for the amount of data that will be sent over your network based on your appliance's camera settings. Note that the file sizes are presented as a range of potential values because the actual size of each file is highly dependant on the amount of detail that is contained in the image.

**Table 2 – Image file sizes based on camera resolution**

Camera Resolution	Maximum Images Captured per Second	Approximate Image Size
160x120	30 frames per second	1.2KB – 5KB
320x240	30 frames per second	8KB – 12KB
640x480	30 frames per second	30KB – 51KB
800x600	10 frames per second	50KB – 73KB
1024x768	10 frames per second	70KB – 114KB
1280x1024	10 frames per second	100KB – 175KB

Appliances that are configured to send surveillance data and security alerts can generate a significant amount of network traffic, especially if the appliance camera is configured to generate high-resolution images at a high frame rate. Also, due to hardware differences on each platform, we suggest a limitation on the number of cameras monitored by the InfraStruXure Central server. **Table 3** shows the suggested limits.

**Table 3 – Surveillance license limitations**

Platform	Surveillance License Limit
Basic	15
Standard	125
Enterprise	250

Of course, how much of an impact this data would have on a network is largely dependent on current network bandwidth utilization, the number of appliances and cameras that are deployed across your network and the amount of activity that is captured and transmitted across the network by the appliances. Frame rates of no more than 5 frames per second are more than adequate for most camera applications. If you require higher frame rates and image resolutions but are concerned about network bandwidth consumption, NetBotz appliances also support the ability to store image data on the devices until it is requested by the InfraStruXure Central server. This can greatly reduce the amount of data transmitted across your network.

## Network time protocol support

InfraStruXure Central is enabled to use public NTP servers to set its own clock and calendar, and can act as an NTP server for supported devices. Managed devices which reside on the network can be configured to automatically obtain their clock and calendar settings from the InfraStruXure Central server.

## SNMP support

InfraStruXure Central 5.x features an SNMP agent. If desired, you can configure InfraStruXure Central to report data to other SNMP-based network management console applications, such as HP OpenView, Tivoli, CA Unicenter, and so on.

## LDAP support

InfraStruXure Central supports LDAP authentication. LDAP support enables you to configure your InfraStruXure Central server to authenticate with an LDAP server (such as Microsoft Active Directory) which will automatically access the permissions for LDAP user accounts when a user logs into InfraStruXure Central.

## Conclusion

InfraStruXure Central automatically discovers supported networked devices in a number of different IP address ranges up to the number of device licenses available. InfraStruXure Central impacts network utilization by varying amounts based on a number of usage factors, many of which can be mitigated by device configuration. InfraStruXure Central also has the functionality to act as an NTP server to the devices it manages.