PLANTSCAPE SERVER

DISTRIBUTED SERVERS ARCHITECTURE

TABLE OF CONTENTS

SESSION OBJECTIVES

At the end of this section of the course the student will be able to:

- Describe the operational effects of using Distributed Servers Architecture
- Configure two or more Servers so that the point data of each Server can be accessed from any other Server
- Describe how alarms are distributed between several servers using Distributed Servers Architecture
- Configure a number of servers to perform specified alarm display and acknowledgement requirements

REFERENCES

Knowledge Builder: Plantscape Server Configuration Guide

Distributed Servers Architecture - Overview

What is Distributed Servers Architecture?

Distributed Servers Architecture enables systems with multiple PlantScape Servers to be connected together in such a way that users can view any point in any Server, regardless of which Server their Station is connected to.

The points which are available in this way require no additional configuration than normal, all the functionality is provided by the Distributed Servers Architecture option.

> **Attention**
>
> Only point details can be accessed remotely using this option. Details about Redundant Servers, Channels, Controllers, Stations, Printers and Connections are not available remotely. If such details are required it is necessary to connect a Station to the appropriate Server.

How are Points viewed?

Points in the database of the Server to which the user is connected are referred to as “local” points.
Points in any other Server to which access has been configured are referred to as “remote” points.

Both local and remote points are displayed as if they are local points, thus there is no operational impact when using this option.

How are Remote Point details accessed?

When a client requests a point that is not in the local Server’s database a request is sent to each remote Server in turn to find who “owns” the point. When the owner is established the point details are retrieved and stored in a local cache.

The data in this cache is then updated on a “report by exception” basis until such time that no clients require the data.

Once an image of a remote point has been established in the cache subsequent requests for data from that point can be responded to much faster as the path to the remote point is already known.

continued on next page

Distributed Servers Architecture – Overview…..continued

What Types of Servers can do this?	Currently only PlantScape Servers at R300 can use this option. These servers can be single or redundant. In the near future the Honeywell Enterprise Buildings Integrator server will also have this option available.
What are the Network Considerations?	This option can use single or dual network connections. It can also work over LANs or WANs. Improved Server connect and reconnect performance will be achieved if the network can support multicasting. Multicasting is not always available as it can have an adverse impact on the network loading. Check with the Network Administrator.

Distributed Servers Architecture - Considerations

Point IDs

Point IDs must be unique across all Servers in a system if they are to be available for remote access.

> **Attention**
>
> If two points with the same Point IDs exist in different remote Servers, a local Server will create a cache entry for the first point that it locates.

Quantity of Points

Remote points are not included in a Server's point count for licensing considerations.

The total number of local plus remote points in a Server cannot exceed 65,000.

Areas

Areas are used to identify the location of points to avoid having to specify a point's local server when access is required.

Area codes must be unique across all Servers in a system.

NT Security

The "mngr" account password MUST be the same on all Servers in the same system.
This will be discussed further in the *Administration and Analysis* section of this course.

Algorithms

It is not possible to view the algorithm details of a remote point.

It is only possible to view algorithm details for local points in the Server to which the user's Station is connected.

Time Synchronisation

All Servers in the same system should have their clocks synchronised even though they might be in different time zones.

This is important for the correct sharing of history data and alarms.

Raise/Lower adjustment of remote variables

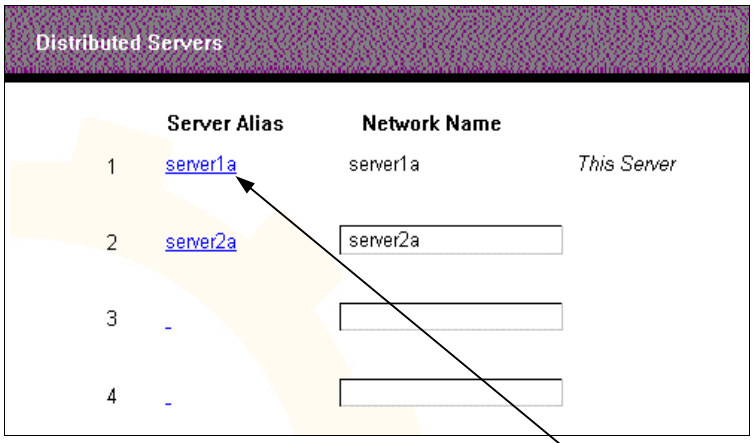
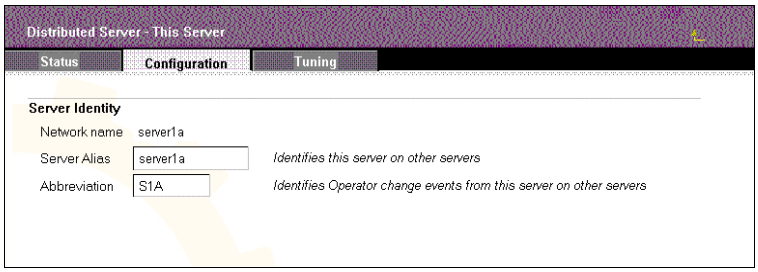
The Distributed Servers Architecture option supports the adjustment of parameters from remote points using the Raise/Lower or
Fast Raise/Fast Lower tools or function keys.

The Fast Raise/Fast Lower step size is determined by the Server to which the user's Station is connected.
This is described in more detail in the *Server Wide Configuration* Section of this course.

Distributed Servers Architecture - Configuration

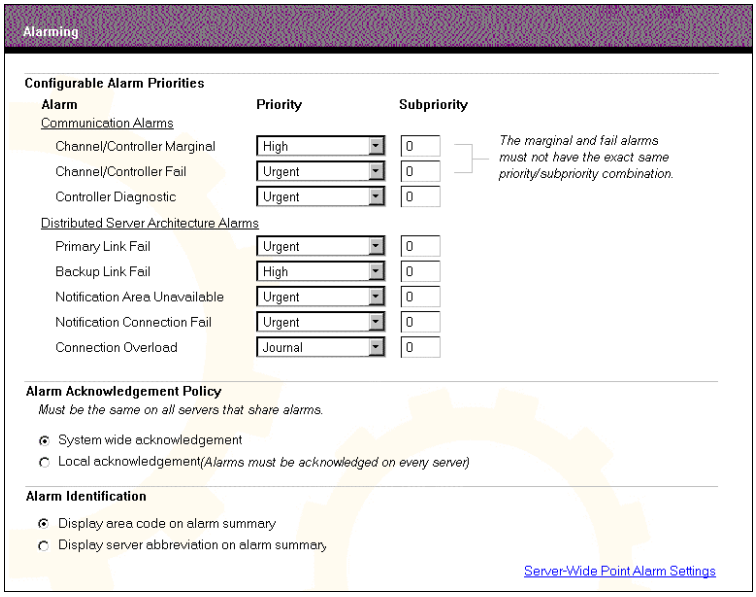
Procedure

The following steps need to be completed on all Servers in a system to enable them to share point data:

Step	Action
1	The Distributed Servers Architecture licence option must be enabled on each Server that will be sharing its local points or accessing remote points. Each Server licence also defines the number of remote Servers from which point data can be accessed.
2	Add an entry to the Hosts file for each Server in the system. Copy this file to each Server in the system.
3	Synchronise the time between each Server in the system using the Windows NT program **timeserv.exe**.
4	Configure each Server from which points will be accessed by choosing **System Configuration⇒Distributed Servers** 
5	Select the Server Alias labelled “This Server” 

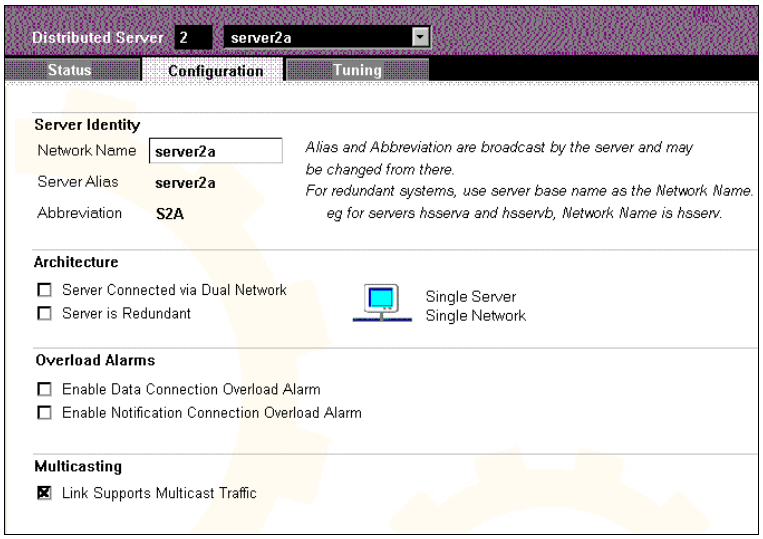
continued on next page

Distributed Servers Architecture – Configuration…..continued

6	The `Network name` field is filled automatically by the Server. The `Server Alias` can be set to any name (16 characters maximum). Use the Network name unless it is a non-meaningful name. The `Abbreviation` is used by remote Servers to reference notifications from "This Server" (5 characters maximum).
7	Choose System **Configuration⇒Alarming** and configure: • The priorities used by various communication alarms on "This Server". • The system Alarm Acknowledgement policy (must be the same on all Servers in the system). • Whether the Alarm Summary on "This Server" identifies the source of point alarms by Area Code or Server Abbreviation. The source of alarms from System Areas in all Servers is always identified by the Server Abbreviation. 

continued on next page

Distributed Servers Architecture – Configuration…..continued

8	Return to the page displayed at step 4 and select the first unconfigured Server Alias in the list 
9	Enter the `Network Name` of another Server, deleting the final A or B in the case of Redundant Servers. The `Server Alias` and `Abbreviation` fields will then be completed automatically. • Configure the appropriate Server and network details for the remote Server. • Configure the appropriate Overload Alarms details for the remote Server. • Specify whether or not the link from “This Server” to the remote Server supports multicasting.
10	Repeat steps 7 and 8 for each remote Server from which points will be accessed.

continued on next page

Distributed Servers Architecture – Configuration…..continued

11	At each Server choose System **Configuration⇒Areas** In addition to all the Areas that have been configured for local points, add to the list all the Areas in remote Servers from which points will be accessed by “This Server”. Choose the correct local Server Alias for each Area. An incorrect selection will result in an alarm when an attempt is made to connect to a point from that Area. Use the **Enable Areas** checkbox to determine which Area alarms will be monitored by “This Server”.