

System 800xA

Network Configuration

System Version 5.1

Power and productivity
for a better world™



System 800xA

Network Configuration

System Version 5.1

NOTICE

This document contains information about one or more ABB products and may include a description of or a reference to one or more standards that may be generally relevant to the ABB products. The presence of any such description of a standard or reference to a standard is not a representation that all of the ABB products referenced in this document support all of the features of the described or referenced standard. In order to determine the specific features supported by a particular ABB product, the reader should consult the product specifications for the particular ABB product.

ABB may have one or more patents or pending patent applications protecting the intellectual property in the ABB products described in this document.

The information in this document is subject to change without notice and should not be construed as a commitment by ABB. ABB assumes no responsibility for any errors that may appear in this document.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license. This product meets the requirements specified in EMC Directive 2004/108/EC and in Low Voltage Directive 2006/95/EC.

TRADEMARKS

All rights to copyrights, registered trademarks, and trademarks reside with their respective owners.

Copyright © 2003-2013 by ABB.
All rights reserved.

Release: February 2013
Document number: 3BSE034463-510 E

Table of Contents

About this User Manual

Feature Pack	14
User Manual Conventions	14
Warning, Caution, Information, and Tip Icons	14
Terminology.....	15
Released User Manuals and Release Notes	18

Section 1 - Introduction

Network Topologies.....	22
Plant Network.....	23
Client/Server Network.....	23
Control Network.....	23
Fieldbus / Field Networks	24
Network Areas.....	24
Combined Client/Server and Control Network.....	25
Client/Server Network and Control Network on Separate Network Areas.....	26
Large Configuration with Control Network on Two Network Areas.....	27
Introduction to Network Redundancy	28
Selecting IP Addresses	29
Recommended IP Address Plan	30
Network plan for field networks	35
Introduction to Domain Controllers	35
Introduction to DNS, Name and Address resolution.....	36

Section 2 - Network Redundancy and Routing

RNRP	37
------------	----

Network Areas.....	38
Fault Handling within a Network Area.....	40
Multiple Network Areas and RNRP Routers.....	41
Local Network Areas.....	47
Building large networks by using Backbone Network Areas.....	47
RNRP Address Configuration: Implicit or Explicit.....	50
Using Explicit RNRP Configuration.....	51
First Project download when using other addresses than 172.16.x.x.....	52
Address Rules for Implicit RNRP Configuration.....	52
RNRP Configuration Parameters.....	54
Mixing Explicit and Implicit RNRP Configuration.....	61
Interconnection of Network Areas over WAN.....	61
Interconnecting RNRP Network Areas via Standard IP Routers.....	62
Use of Layer 2 VPN Solutions.....	66
Use of Layer 3 VPN Solutions.....	67
RNRP in a PC.....	67
Configuring a Network Adapter.....	67
Installing RNRP.....	68
Configuring RNRP in a PC.....	69
Verify RNRP Connectivity.....	70
Configuring what Networks to Use.....	71
RNRP Network Loop Detection and Protection.....	72
 Section 3 - Distributed System Topologies	
Extend the 800xA Automation System Network.....	74
Equal System Sections on Different Locations.....	78
Security Considerations.....	79
Multisystem Integration.....	80
Multisystem Integration with redundancy.....	82
Asset Optimization.....	83
 Section 4 - Field Networks	
Selecting IP Addresses for Field Networks.....	86

Field Network Connectivity Servers88
 Routing from the system network 88
 Network Redundancy89
 Physical Field Networks90
 Protocol specific documentation90

Section 5 - Network Security

Establish a Network Security Policy91
 The Onion Approach92
 Firewalls94
 Connections to 800xA Systems through Firewalls.....96
 Connect Inside-out Instead of Outside-in96
 Network Address Translation in Firewalls.....96
 Single Firewall or a Demilitarized Zone99
 Connecting a single Firewall to a Redundant Network..... 104
 Using an Extra Network for Remote Access 105
 Redundant connection to external network 106
 Virtual Private Networks (VPN) for Secure Connections..... 106
 Use cases for Connections through Firewalls..... 108
 Remote/External Client 109
 Remote Windows Workplace 110
 Remote Usage of a Node on the System Network 110
 Information Manager Desktop Tools 111
 Secure Connections for Remote Clients 111
 Remote Clients Connecting through a Demilitarized Zone 112
 Site to Site Connections via a Firewall..... 112
 Integration with 3rd Party Systems 113
 Accessing OPC Data from External Network..... 114
 Asset Optimization Integrations..... 116
 Batch Integrations 117
 Management of System Updates 117
 Using WSUS for Windows Updates 118
 Using ePO for McAfee updates 119

Other Services to be Used Through a Firewall 119
Summary of Ports to Open in Firewalls 120
AC 800M Network Storm Protection..... 121

Section 6 - Domain Setup and Name handling

Node name handling and DNS..... 123
 Choosing Names for Domains and PCs..... 123
 Allocating 800xA Systems to Domains 124
Configuring Name Resolution and DNS..... 125
Which Nodes use host names..... 125
Location of Domain Controllers 126
Maintaining Redundant Domain Controllers 126
 DcDiag: Domain Controller Diagnostics..... 126
 Backups of Domain Controllers 126
 Recovering after a Crash of the First Installed Domain Controller 127
Time Synchronization in a Domain..... 129
DNS Server Configuration 129
DNS Configuration in Each Node..... 132
 General DNS configuration in each node 132
 RNRP's host file service 135
 Configuring the Order of the Network Interfaces 137
Windows Workgroups instead of Windows Domain 138
Example of IP Addresses and DNS Configuration 139
Verifying Name Resolution functions 142
 The RNRP monitor shows node names 142
 ping -a instead of nslookup..... 142
 Special Considerations when Changing DNS Configuration 142

Section 7 - Time Synchronization

Recommended Time Synchronization Schemes 146
 Local Time Source..... 146
 External Time Source..... 150
 Windows Time Instead of AfwTime..... 153

Systems with More Than One Control Network.....	156
Time Synchronization with Multisystem Integration.....	157
Systems with MB 300 and 800xA for AC 800M.....	160
MB 300 as Time Source for AC 800M.....	164
Synchronization from the Client Server Network.....	167
Systems with AC 800M HI with Safe Peer-To-Peer.....	170
Configure Time Synchronization in Controllers.....	171
Time Synchronization Parameters for AC 800M.....	171
Time Synchronization for MB 300 via CI855.....	173
Time Synchronization in Advant Master Controllers.....	174
CNCP - Control Network Clock Protocol.....	174
Forwarding of CNCP Between Network Areas.....	176
SNTP - Simple Network Time Protocol.....	176
SNTP Implementations.....	176
Stratum.....	177
SNTP Servers on a Redundant Network.....	177
Routing SNTP Traffic.....	178
Configuring SNTP.....	178
MB 300 Time Synchronization.....	178
MMS Time Synchronization.....	180
AfwTime Service.....	180
Configuration of the AfwTime Service.....	182
Configuring the AfwTime Server and the Server Group.....	184
Configuring an AfwTime Client.....	186
Time Synchronization for Connectivity Servers, Time Adaptors.....	188
AC 800M Time Adaptor.....	189
Advant Master Time Adaptor.....	189
Time Synchronization on the RTA Board.....	190
Time Sync with 800xA for Harmony.....	192
Time Sync with 800xA for Melody.....	193
Time Sync with 800xA for MOD 300 and 800xA for DCI.....	193
Windows Time Service (W32Time).....	194

Disable/Enable the Windows Time Service.....	195
Configuring Time Zone and Daylight Saving Time Support.....	196
Enable the SNTP Server, Disable SNTP Client in a PC.....	196
Configure Time Synchronization in a Dedicated Domain Controller	197
Comparison Between W32Time and the AfwTime Service.....	198
Tuning the Synchronization Rate for W32Time	199
Setting the System Time.....	199
Setting the Time with CNCP using the Control Builder M	202
Setting the time for the AfwTime Service	203
Adjust the Time in AC 800M via the Function Block SetDT.....	204
Handling Time Changes when Using W32Time	205
Adjusting Time with 800xA for Melody or 800xA for Harmony	206
Fault Tracing Time Synchronization Problems.....	206
Fault Tracing Time Sync in Controllers.....	206
Fault Tracing SNTP	208
Fault Tracing AfwTime.....	208

Section 8 - Ethernet and Network Equipment

Building a Physical Network.....	211
Hubs and Switches	212
Features in Switches.....	213
Managed Switches	213
Basic Requirements on Switches	214
Necessary settings in Managed Switches	214
Features not Required in Switches.....	215
Recommended Features in Switches	215
Ethernet Speed	215
Testing network performance	216
Physical Network Installation	216
Coexistence of Network Types	218
Reducing HW using Virtual LANs.....	219
Ring Redundancy.....	220
Using Rapid Spanning Tree	222

Environmental Consideration.....	224
Connecting to a Redundant Network.....	227
Connecting a PC.....	228
Connecting a Controller without CPU Redundancy	228
Connecting a Controller with CPU Redundancy	229
Routers.....	230

Section 9 - Network Monitoring and Maintenance

System Status Viewer	231
Afw Service Connection Status Viewer	234
Topology Designer / Topology Status Viewer.....	235
Node Status Alarms	236
Ping	237
RNRP Network Monitor.....	237
RNRP Events in Controllers	239
RNRP Fault Tracer/RNRP Utility	239
Network Interface Supervision in a PC	240
Network Interface Supervision in a Controller.....	241
Monitoring MMS Communication.....	243
Using Network Management information.....	244
PC, Network and Software Monitoring.....	244
Network Management Tools from Switch Vendors	246

Appendix A - Reference Details

IP Addresses	247
How to Choose IP Addresses	249
Choosing Address Space.....	249
Using Implicit or Explicit RNRP Configuration.....	250
Suggested Configuration of RNRP and IP Addresses	251
IP Addresses for Redundant Controller Nodes	252

Index

Revision History

Updates in Revision Index A..... 258
Updates in Revision Index B..... 258
Updates in Revision Index C..... 258
Updates in Revision Index D..... 259
Updates in Revision Index E..... 260

About this User Manual



Any security measures described in this document, for example, for user access, password security, network security, firewalls, virus protection, etc., represent possible steps that a user of an 800xA System may want to consider based on a risk assessment for a particular application and installation. This risk assessment, as well as the proper implementation, configuration, installation, operation, administration, and maintenance of all relevant security related equipment, software, and procedures, are the responsibility of the user of the 800xA System.

This manual describes how to configure the 800xA Automation System Network, including the Client Server Network, the Control Network, and how to connect to a Plant Network. It generally does not cover fieldbuses.

The section about Network equipment however applies to Ethernet communication in general, which means that it also applies to Fieldbuses using Ethernet.

For the 800xA Automation System network the following main topics are covered:

- System Network topologies
- Network Redundancy
- Domain and DNS configuration
- Clock Synchronization
- Network installation and maintenance
- Network Security

[Section 1, Introduction](#) introduces the topics and the following sections describe them in more details.

For configuration of users, user groups, security settings, and group policies, please refer to *System 800xA Administration and Security (3BSE037410*)*.

This manual does not describe configuration of general purpose networks, such as

an office or plant network, neither does it cover the situation where 800xA products are connected to a general purpose network.

Feature Pack

The Feature Pack content (including text, tables, and figures) included in this User Manual is distinguished from the existing content using the following two separators:

Feature Pack Functionality

<Feature Pack Content>

Feature Pack functionality included in an existing table is indicated using a table footnote (*):

*Feature Pack Functionality

Feature Pack functionality in an existing figure is indicated using callouts.

Unless noted, all other information in this User Manual applies to 800xA Systems with or without a Feature Pack installed.

User Manual Conventions

Microsoft Windows conventions are normally used for the standard presentation of material when entering text, key sequences, prompts, messages, menu items, screen elements, etc.

Warning, Caution, Information, and Tip Icons

This manual includes **Warning**, **Caution**, and **Information** where appropriate to point out safety related or other important information. It also includes **Tip** to point out useful hints to the reader. The corresponding symbols should be interpreted as follows:



Electrical warning icon indicates the presence of a hazard which could result in *electrical shock*.



Warning icon indicates the presence of a hazard which could result in *personal injury*.



Caution icon indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard which could result in *corruption of software or damage to equipment/property*.



Information icon alerts the reader to pertinent facts and conditions.



Tip icon indicates advice on, for example, how to design your project or how to use a certain function

Although **Warning** hazards are related to personal injury, and **Caution** hazards are associated with equipment or property damage, it should be understood that operation of damaged equipment could, under certain operational conditions, result in degraded process performance leading to personal injury or death. Therefore, **fully comply** with all **Warning** and **Caution** notices.

Terminology

A complete and comprehensive list of terms is included in *System 800xA System Guide Functional Description (3BSE038018*)*. The listing includes terms and definitions that apply to the 800xA System where the usage is different from commonly accepted industry standard definitions and definitions given in standard dictionaries such as *Webster's Dictionary of Computer Terms*.

Terms that uniquely apply to this manual are listed in the following table.

Term/Acronym	Description
AC 800M HI	AC 800M High Integrity controller, certified for SIL 2 safety applications
Afw Services	A system service for the 800xA core system
Client	Client is a part of a software that subscribes data from a server.
Client/Server Network	A client/server network is used for communication between servers, and between workplaces and servers.
CNCP	Control Network Clock Protocol. An ABB protocol for synchronization of clocks in Controllers on the Control Network.
Connectivity Server	A server that provides access to controllers and other sources for real-time data, historical data, and alarm and event data. A Connectivity Server runs services related to OPC/DA, OPC/AE, OPC/HDA.
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FSMO role	Flexible Single Master Operation role. An Active Directory role which is not bound to a single Domain Controller
Hop count	A measure of distance in a network. The hop count is equal to the number of routers that must be passed to reach a destination.
IAC	Inter Application Communication (between AC 800M controllers)
IP	Internet Protocol. A layer 3 protocol in the OSI model.
IP address	A 32-bit address assigned to each host/node connected on the network.

Term/Acronym	Description
IP address mask	A 32-bit address mask used on an IP address to separate network from host identifier.
IPsec	Internet Protocol Security
LAN	Local Area Network
Mbps	Mega Bit Per Second
MMS	Manufacturing Message Specification. ISO standard for communication between controllers.
MPLS	Multi Protocol Label Switching
Node	A computer communicating on a network e.g. the Internet, Plant, Control or I/O network. Each node typically has a unique node address with a format depending on the network it is connected to.
OSPF	Open Shortest Path First
PC	Computer running the Windows operating system
Private IP addresses	Blocks of IP address space that are reserved by the Internet Assigned Numbers Authority (IANA) for free use in private networks.
RMON	Remote Monitoring. A standard for performing traffic analysis
RNRP	Redundant Network Routing Protocol
Router	A computer/device that forwards IP datagrams among the networks to which it is connected
SattBus	An ABB fieldbus
Server	A node that runs one or several Afw Services. It is the part of the software that supply data to a subscriber.
SIL	Safety Integrity Level
SNMP	Simple Network Management Protocol

Term/Acronym	Description
SNTP	Simple Network Time Protocol
STP	Shielded Twisted Pair cable
TCP	Transmission Control Protocol. A Transport Layer protocol in the Internet Protocol Suite
UDP	User Datagram Protocol. A Transport Layer protocol in the Internet Protocol Suite
UTC	Coordinated Universal Time
UTP	Un-shielded Twisted Pair cable
WAN	Wide Area Network
VLAN	Virtual Local Area Network
WLAN	Wireless Local Area Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol

Released User Manuals and Release Notes

A complete list of all User Manuals and Release Notes applicable to System 800xA is provided in *System 800xA Released User Manuals and Release Notes (3BUA000263*)*.

System 800xA Released User Manuals and Release Notes (3BUA000263)* is updated each time a document is updated or a new document is released.

It is in pdf format and is provided in the following ways:

- Included on the documentation media provided with the system and published to ABB SolutionsBank when released as part of a major or minor release, Service Pack, Feature Pack, or System Revision.

- Published to ABB SolutionsBank when a User Manual or Release Note is updated in between any of the release cycles listed in the first bullet.



A product bulletin is published each time *System 800xA Released User Manuals and Release Notes (3BUA000263*)* is updated and published to ABB SolutionsBank.

Section 1 Introduction

This section introduces the main areas covered by this document:

- Network Topologies, on [page 22](#).
- Network Redundancy, on [page 28](#).
- Selection of IP addresses, on [page 29](#).
- Domain Controllers, on [page 35](#).
- DNS configuration and Name handling, on [page 36](#).

The later sections will describe the different topics in detail.

Network Topologies

System communication in System 800xA is based on Ethernet and TCP/IP networks, which are functionally and, in most cases, also physically built in levels.

The following figure shows the different levels in the network. Later sections will describe more about why the system should be separated into different network areas on different levels.

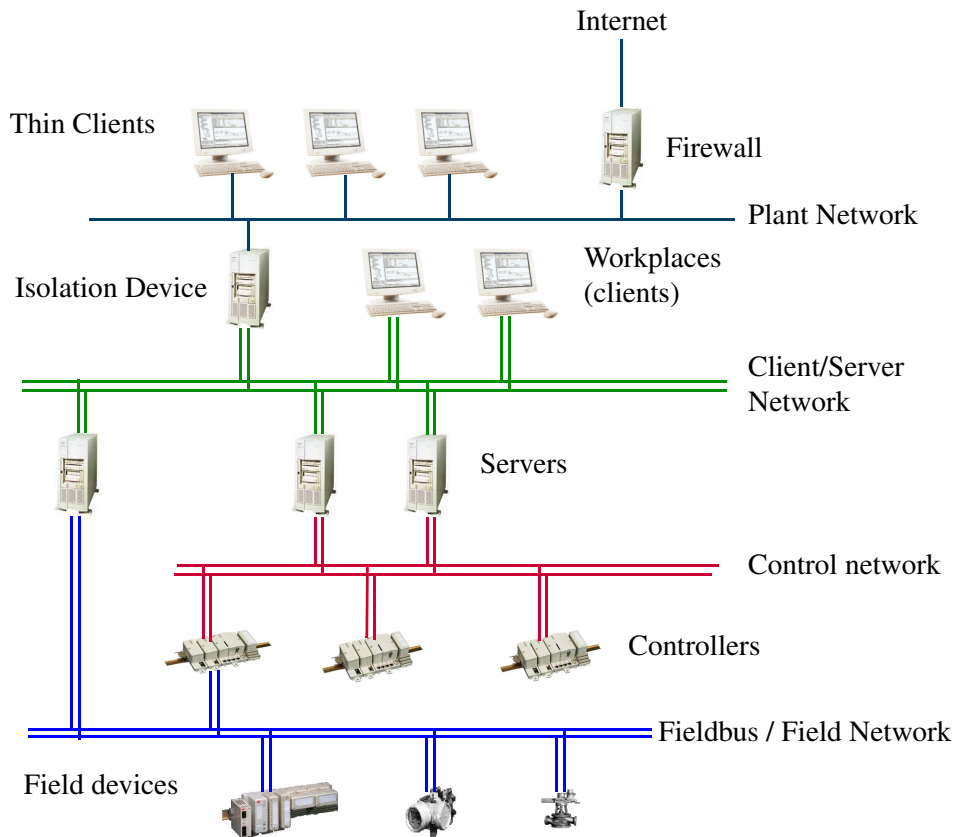


Figure 1. Network Topology: Plant-, Client/Server- and Control Network

Plant Network

The Plant Network can be dedicated for process automation purposes or be a part of the plant intranet already available on a site.

Client/Server Network

The Client/Server network is used for communication between servers and between client Workplaces and servers.

The Client/Server Network is a trusted network zone that should be protected by firewalls. It is a private IP network that uses static addresses, see the recommendations on [Selecting IP Addresses](#) on page 29.

The Client/Server Network supports network redundancy using the RNRP protocol and redundant Ethernet switches. Server and client PCs need additional network cards to adapt to redundant networks.



Due to security and performance reasons only Industrial^{IT} Certified products should be connected on the Client/Server Network.

Control Network

The Control Network is used for communication between Controllers and between Controllers and Connectivity Servers. The Control Network is a trusted network zone that should be protected by firewalls. It is a private IP network that uses static addresses, see the recommendations on [Selecting IP Addresses](#) on page 29.

The maximum number of nodes on a Control Network area is 60 if any AC 800M with the processor modules PM85x or PM86x is connected to the network. If only PM89x is used the limit is 100.

The Control Network is based on Ethernet using the MMS protocol on top of a TCP/IP protocol stack, plus additional services for time distribution, redundancy management, etc. The Control Network supports network redundancy using the RNRP protocol and redundant Ethernet switches. Controllers connect to the control network via dual built-in network ports.



The Control Network should only be used for Controller traffic. Other traffic, especially broadcast or multicast traffic, may jeopardize Controller performance.

Connect only Industrial^{IT} Certified products to the Control Network.

Fieldbus / Field Networks

System 800xA supports a large number of Fieldbuses. Some of these are based on Ethernet and are in this document referred to as Field Networks.

The specification for the specific Field Network describes the nodes to be connected to the network. This may include sensors, activators, IO systems, motor control systems, electrical protection relays, gateways and so on. These may be from ABB or 3rd party suppliers.

Out of the 800xA node types Controllers and Connectivity Servers connect to field networks.

It is recommended that separate networks be built for these protocols, i.e. avoid combining a Field Network with the Control Network. For more information see [Section 4, Field Networks](#).

Network Areas

The terms Client/Server Network and Control Network are used to describe the system functions performed by these networks. From an IP routing point of view the concept of Network Areas is used. A Network Area is a logically flat network that does not contain IP routers, i.e. routers can not forward traffic from one to another place on the same network area. In [Figure 1](#), the Client/Server Network and the Control Network are different Network Areas with the Connectivity Servers potentially being used as IP routers. A Network Area may be redundant or non-redundant. A non-redundant Network Area maps to one IP subnet. A redundant Network Area maps to two IP subnets.

Combined Client/Server and Control Network

In systems where the number of nodes is within the limit for the Control Network the Client/Server Network and the Control Network may be combined to one network.

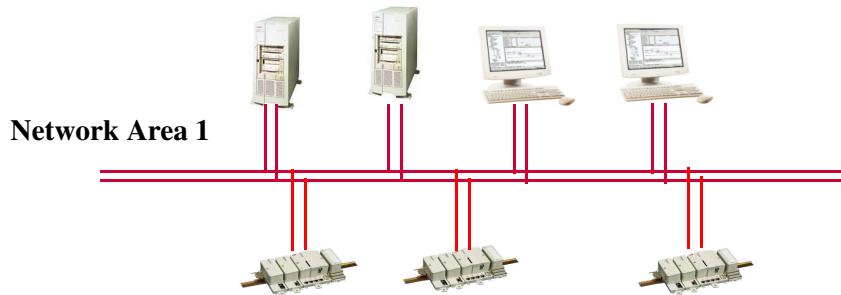


Figure 2. Combined Control Network and Client/Server Network

Client/Server Network and Control Network on Separate Network Areas

For medium to large systems it is recommended that the Control Network and Client/Server Network be separated into different Network Areas. The connection between the Network Areas is provided by Connectivity Servers using the RNRP routing protocol ([Section 2, Network Redundancy and Routing](#)). The two networks may be separated also for smaller systems. There are several reasons to separate the Control Network from the Client/Server Network:

- Fault isolation. An erroneous network segment on Client/Server Network will not affect nodes on the Control Network.
- Limitation of broadcast traffic. Broadcasts on Client/Server Network will not disturb the real-time traffic on the Control Network
- Traffic filtering. Undesired traffic can be blocked by the Connectivity Servers. The Control Network is more secure if it is isolated from the Client Server Network

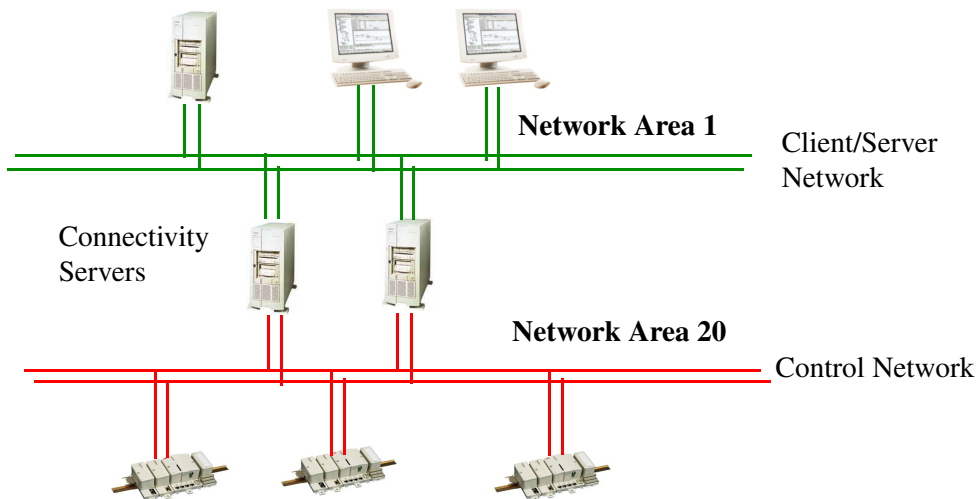


Figure 3. Separated Client Server Network and Control Network

Large Configuration with Control Network on Two Network Areas

If the number of Control Network nodes is more than the limit for a Control Network area it is recommended to split the Control Network on two or more Network Areas.

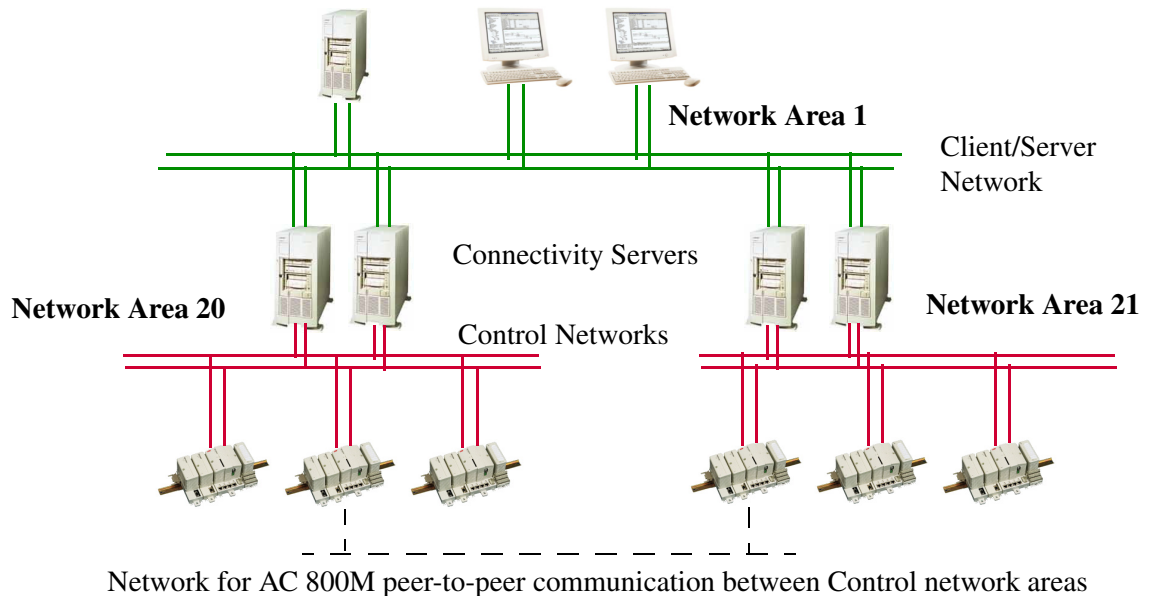


Figure 4. Separated Client Server Network and Multiple Control Networks

For best performance the controller to controller communication should be kept within one Network Area.

Controllers on different Network Areas can communicate with MMS and IAC through the Client/Server Network, area 1 in the example above. The Connectivity Servers will act as routers, see [Connectivity Servers as Routers](#) on page 42.

Communication between controllers on different network areas can also be done using a protocol provided by any of the CI modules connected to AC 800M, e.g. MB 300 via CI855 or one of the fieldbuses. *System 800xA, AC 800M, Communication Protocols (3BSE035982*)* gives a complete overview of the options.

Introduction to Network Redundancy

For high availability, all network devices (cables, switches, routers and network adapters) should be duplicated in physically separated network paths. The two network paths are named Primary Network and Secondary Network.

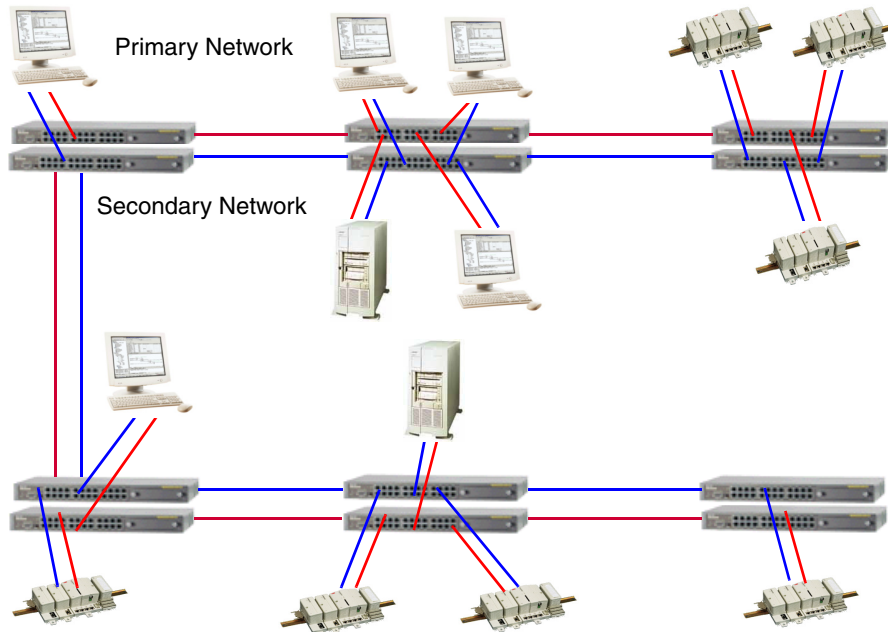


Figure 5. Physical View of a full Redundant Network with Duplication of Switches, Cabling and Network Adapters

As long as the primary network paths are working, all process data is sent on that network. The secondary network normally carries no user traffic. This guarantees that network performance is not affected after a network fail over.

Both supervision of network paths and fail-over between Primary and Secondary networks are performed by RNRP.

In order to have a robust redundant system, it is very important to have continuous supervision of all network paths on a node-to-node basis, not only on individual

network devices. A detected network error results in fault annunciation. See [Section 9, Network Monitoring and Maintenance](#).

For more information about redundancy, RNRP and network configurations, please read [Section 2, Network Redundancy and Routing](#).

[Section 4, Field Networks](#) describes redundancy for Field networks not using RNRP.

Selecting IP Addresses

When planning a system the user must decide what IP addresses to use for all nodes in the system.

It is recommended that addresses be selected from a private address space.

This has the following advantages:

- There is no requirement to apply to the licensing authorities for an IP address, i.e. it is easy to allocate a large IP address space especially in redundant network configurations.
- Some protection is gained against illegal access because private addresses are not permitted on the public Internet.



It is strongly recommended that addresses shown in the next chapter are used. This greatly simplifies the network configuration and reduces the probability for configuration errors.

If it is not possible to use the recommended IP addresses, then read about RNRP addresses in [RNRP Address Configuration: Implicit or Explicit](#) on page 50 and in Appendix A [How to Choose IP Addresses](#) on page 249.

Recommended IP Address Plan

This section gives a recommendation on IP addresses that will work for most installations. If this suggestion is followed, the reader can disregard much of the details about RNRP configuration. [Table 1](#) suggests which NetIDs¹ to use.

Table 1. Suggested NetIDs and Network Area Numbers

Network type	NetIDs	Network Areas
Plant Network	172.16.0.0 172.17.0.0	0
Client/Server Networks	172.16.x.0 172.17.x.0 where x=4,8,12 to 36 (steps of 4)	1-9
RTA Units PU410 and PU412	172.16.168.0 172.17.168.0	10
Control Networks	172.16.x.0 172.17.x.0 where x=80, 84, 88 to 124 (steps of 4)	20-31

Use the subnet mask 255.255.252.0 for all network interfaces.

See also [Network plan for field networks](#) on page 35.



Do not connect more than 50 nodes to a Control Network Area where AC 800M controllers with processor modules PM85x or PM86x are used.

If only PM891 is used 100 nodes can be connected to the Control Network.

1. NetID is the left most part of the IP address. See [Appendix A, Reference Details](#)



For the node status alarms to work properly node numbers must uniquely identify a node within the whole network. Two different nodes are not allowed to use the same node number even if they are located on different network areas and even if they belong to different 800xA Systems.

A node which is connected to more than one RNRP network area must use the same node number on all its areas. This for example means that:

- Two Controllers on two different Control Networks must use different node numbers, e.g. 151 and 201.
- A Client on the Client Server Network and a Controller on the Control Network must use different node numbers, e.g. 150 and 151.
- A Connectivity Server must use the same node number, e.g. 21, on the Client Server Network and the Control Network

If this rule is not followed the consequence is that if one node is disconnected from the network the alarm list may indicate that another node (one with the same node number) was disconnected.

Addresses recommended on the Client/Server/Control Network Area 1

Table 2. Suggested Addresses for Nodes on Network Area (1)

Nodes	Node number	Addr on Primary Network	Addr on Secondary Network
Domain and DNS servers	1-10	172.16.4. 1 - 172.16.4.10	172.17.4. 1- 172.17.4.10
Aspect servers	11-20	172.16.4.11 - 172.16.4.20	172.17.4.11- 172.17.4.20
Connectivity servers	21-50	172.16.4.21 - 172.16.4.50	172.17.4.21 - 172.17.4.50
Application Servers IM, Batch, 3rd party	51-70	172.16.4.51- 172.16.4.70	172.17.4.51 - 172.17.4.70
Workplace Clients	71- 150	172.16.4.71 - 172.16.4.150	172.17.4.71 - 172.17.4.150
Controllers	151-220/255	172.16.4.151 - 172.16.4.220/255	172.17.4.151 - 172.17.4.220/255
Panel 800 (if used) (non redundant)	221-255	172.16.4.221 - 172.16.4.255	(not used)
Backup CPUs for Redundant Controllers	663-767	172.16.6.151 - 172.16.6.255	172.17.6.151 - 172.17.6.255
Switches, Gateways, Firewalls (not RNRP addresses)	(501-511) (1013-1022)	172.16.5.245- 172.16.5.255 172.16.7.245- 172.16.7.254	172.17.5.245 - 172.17.5.255 172.17.7.245 - 172.17.7.254
Spare, Unused RNRP addresses	256-500	172.16.5.0- 172.16.5.244	172.17.5.0- 172.17.5.244
Spare, e.g. printers (not RNRP addresses)	(513 ⁽¹⁾ -662) (768-1012)	172.16.6.1 ⁽¹⁾ - 172.16.6.150 172.16.7.0- 172.16.7.244	172.17.6.1 ⁽¹⁾ - 172.17.6.150 172.17.7.0- 172.17.7.244

(1) IP addresses x.x.6.0 may normally also be used but some nodes do not accept it.

The following addresses are recommended on the Control Network Area 20.

Table 3. Suggested Addresses for nodes on Network Area (20)

Nodes	Node number	Addr on Primary Network	Addr on Secondary Network
Connectivity servers	21-50	172.16.80.21 - 172.16.80.50	172.17.80.21 - 172.17.80.50
Controllers	151-220/255	172.16.80.151 - 172.16.80.220/255	172.17.80.151 - 172.17.80.220/255
Panel 800 (if used) (non redundant)	221-255	172.16.80.221 - 172.16.80.255	(not used)
Backup CPUs for Redundant Controllers	663-767	172.16.82.151 - 172.16.82.255	172.17.82.151 - 172.17.82.255
Switches, Gateways, Firewalls (not RNRP addresses)	(501-511) (1013-1022)	172.16.81.245- 172.16.81.255 172.16.83.245- 172.16.83.254	172.17.81.245 - 172.17.81.255 172.17.83.245 - 172.17.83.254
Spare, Unused RNRP addresses	256-500	172.16.81.0- 172.16.81.244	172.17.81.0- 172.17.81.244
Spare (not RNRP addresses)	(512-662) (768-1012)	172.16.82.0- 172.16.82.150 172.16.83.0- 172.16.83.244	172.17.82.0- 172.17.82.150 172.17.83.0- 172.17.83.244



For controllers running SattBus on TCP/IP the HostID must be 2-127. This means that the user needs to decide on a different node number allocation than [Table 3](#). SattBus is described in the OnLine help for the Control Builder.

The same information as in the previous tables, but generic for any Network Area with the area number as parameter 'a', is shown below (a = [0..31]).
The previous tables represent a=1 and a=20.

Table 4. Suggested Addresses for nodes on a Network Area (a)

Nodes	Node number	Addr on Primary Network	Addr on Secondary Network
Domain and DNS servers	1-10	172.16.4*a. 1 - 172.16.4*a.10	172.17.4*a. 1- 172.17.4*a.10
Aspect servers	11-20	172.16.4*a.11 - 172.16.4*a.20	172.17.4*a.11- 172.17.4*a.20
Connectivity servers	21-50	172.16.4*a.21 - 172.16.4*a.50	172.17.4*a.21 - 172.17.4*a.50
Application Servers IM, Batch, 3rd party	51-70	172.16.4*a.51- 172.16.4*a.70	172.17.4*a.51 - 172.17.4*a.70
Workplace Clients	71- 150	172.16.4*a.71 - 172.16.4*a.150	172.17.4*a.71 - 172.17.4*a.150
Controllers	151-220/255	172.16.4*a.151 - 172.16.4*a.220/255	172.17.4*a.151 - 172.17.4*a.220/255
Panel 800 (if used) (non redundant)	221-255	172.16.4*a.221 - 172.16.4*a.255	(not used)
Backup CPUs for Redundant Controllers	663-767	172.16.4*a+2.151 - 172.16.4*a+2.255	172.17.4*a+2.151 - 172.17.4*a+2.255
Switches, Gateways, Firewalls (not RNRP addresses)	(501-511) (1013-1022)	172.16.4*a+1.245- 172.16.4*a+1.255 172.16.4*a+3.245- 172.16.4*a+3.254	172.17.4*a+1.245 - 172.17.4*a+1.255 172.17.4*a+3.245 - 172.17.4*a+3.254
Spare, Unused RNRP addresses	256-500	172.16.4*a+1.0- 172.16.4*a+1.244	172.17.4*a+1.0- 172.17.4*a+1.244
Spare (not RNRP addresses)	(513-662) (768-1012)	172.16.4*a+2.1- 172.16.4*a+2.150 172.16.4*a 3.0- 172.16.4*a+3.244	172.17.4*a+2.1- 172.17.4*a+2.150 172.17.4*a+3.0- 172.17.4*a+3.244

Network plan for field networks

In addition to the protocols on the System Network an 800xA system may use several other protocols based on Ethernet and TCP/IP, e.g. FOUNDATION Fieldbus, Modbus TCP, IEC 61850 or PROFINET. The system planning needs to include a plan for the networks used for these protocols including for example the addresses ranges to use. [Section 4, Field Networks](#) includes more information on what to consider.

Introduction to Domain Controllers

A domain is a group of nodes that are part of a network and share a common directory database.

A domain defines a scope or unit of policy. A Group Policy object establishes how domain resources can be accessed, configured, and used. These policies are applied only within the domain and not across domains. Applying a Group Policy object to the domain consolidates resource and security management.

A Domain Controller contains matching copies of the user accounts in a given domain. It is used to store and manage information about user credentials and access rights, both for humans and for the system. The Domain Controller provides the Active Directory service that manages user access to a network, which includes user logon, authentication, and access to the directory and shared resources.

Every domain must have at least one Domain Controller. To improve the availability of the system a domain may have multiple Domain Controllers to support the handling of logon requests and directory updates.

The domains are stored in the Active Directory. Administration of Domain Controllers to great extent means administration of the Active Directory. Use Windows Server 2008 on all Domain Controllers in the same domain.



Single node systems, i.e. systems with only one PC, and small systems that use Windows Workgroups do not need Domain Controllers.

Introduction to DNS, Name and Address resolution

DNS (Domain Name System) is a hierarchical name service for domains and IP addresses. The DNS service enables client nodes on your network to register and resolve DNS domain names and to find Domain Controller services.

DNS can be used for finding the IP address of a node which is only known by name (address resolution) and for finding the name of a node which is known by IP address (name resolution).

DNS can also be used for finding Domain Controller services, i.e. which node runs a certain service for the Domain.

In System 800xA 5.1, DNS is only used normally for locating domain controller services. Name and address resolution is performed using hosts files that are updated by RNRP.

800xA applications that identify other nodes by name, i.e. not only by IP Address, use the information from the hosts file to find the corresponding IP address.

Normally the primary (DNS) server is run on the same node as the Domain controller. With multiple Domain Controllers in a system the DNS server functions are also distributed. This also improves the availability of the DNS.

Configuring the DNS functions in a system comprises:

- Configuring the DNS server on the Domain Controller(s).
- Configuring names and IP addresses, for nodes that will be possible to identify by name, in the DNS database.
- Configuring knowledge of the domain and the DNS server(s) in each node that uses DNS.
- Configuring knowledge of the Domain Controllers.

Further information about DNS can be found in the On-line help for DNS in Windows Server, the help file `dnsconcepts.chm` and in the resource kits in MSDN.

[Section 6, Domain Setup and Name handling](#) describes how to configure DNS.

Section 2 Network Redundancy and Routing

This section describes the Network Redundancy based on RNRP (Redundant Network Routing Protocol). The main areas covered are:

- the concepts of the RNRP protocol
- how to build different network structures
- how to choose addresses
- how to configure RNRP in nodes; PCs and Controllers

RNRP

RNRP is an IPv4 routing protocol developed by ABB. It is specially designed for use in automation networks with limited topology but with high demands on network availability. RNRP provides the following features:

- Network redundancy
The protocol supports redundant physical networks, full redundancy including network interface boards, between end nodes. Routing messages are periodically sent as multicast on all networks. If a network error occurs, RNRP updates the IP Routing Table of each affected node with a replacement network path within the “RNRP send period”, a configurable parameter (default=1s).
- Routing between network areas
IP routes to all neighbor nodes and subnetworks are automatically maintained in the IP Routing Table in every node. A node with RNRP can act as an IP router and forward messages on best path to destination nodes.
- Node and network supervision
RNRP quickly detects if a node or remote network is down and sends this information to applications that subscribe to RNRP status. This information is used to detect if a redundant server is down and whether a new server can be connected.

The RNRP redundancy concept works with standard network devices (hubs, switches or bridges) and no special functionality is required from the network interface cards (NICs).

The protocol gives high flexibility to integrate networks with different types of data links like PPP and Ethernet. The routing update period can be configured to fit on very slow serial links as well as on high speed networks mixed in the same Control Network.



IP routing works for Unicast communication (node to node), not for Multicast or Broadcast. This means that RNRP does NOT provide redundancy or routing for Multicast or Broadcast communication.

Applications that use Multicast or Broadcast must take care of the network redundancy themselves, if desired communication between different network areas.



All RNRP versions used in previous system versions of the 800xA System are compatible with each other.

Network Areas

A network that uses RNRP is built up by one or more Network Areas.

A Network Area is a logically flat network structure without routers. Routers are not allowed within a Network Area.

A Network Area with redundancy contains two independent IP networks with equal capacity. The individual networks within a Network Area are assigned Path Numbers.

The primary network has Path Number = 0 and the secondary network has Path Number = 1.

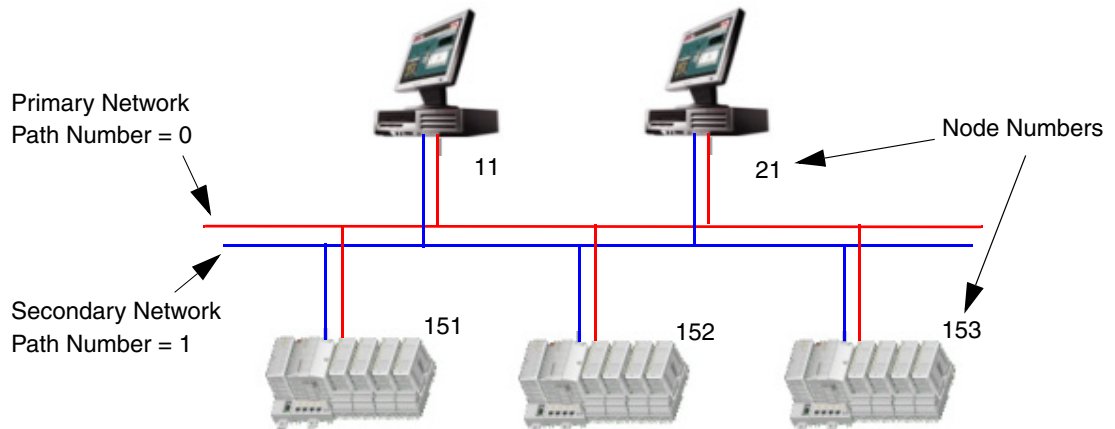


Figure 6. A Network Consisting of one Network Area

A node is identified in RNRP by:

- Network area number (0 - 35)
- Node number (1 - 500)

The path number is a parameter on each network interface (see [RNRP Address Configuration: Implicit or Explicit](#) on page 50).



Each path on a Network Area corresponds to one IP subnet. The NetID is the same for all interfaces on the same Path. (see [IP Addresses](#) on page 247)



Applications communicating with nodes that run RNRP shall always address the nodes on the primary network (path 0).

In case of error on the primary network, the Redundant Network Routing Protocol (RNRP) redirects traffic over to the secondary network (the backup network) without involving any application program.

Nodes with redundant interfaces and nodes with a single interface can be mixed on the same Network Area. A node with only one interface must only be connected to the primary network.

Fault Handling within a Network Area

Within a Network Area RNRP can handle single network errors in all node-to-node connections. In the example below, node A has an error on the connection to the primary network and node B an error on the connection to the secondary network.

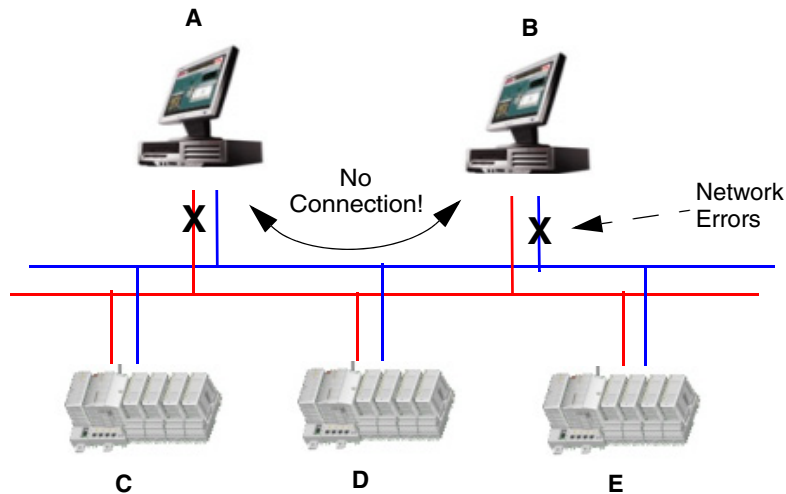


Figure 7. A Fault handling in one Network Area

In this example communication between node A and node B is not possible but all other peer communication will work.

Node A can communicate over secondary network with nodes C, D and E.
 Node B can communicate over primary network with nodes C, D and E.
 Nodes C, D and E are fully redundant to each other.

Network Fail Over Time

The time required for RNRP to redirect traffic from a faulty path to a good path is the same as the configured RNRP parameter **Send Period**, see [Table 5](#) on [page 55](#) (normally 1s).

Data Recover Time

The application data recover time is not the same as the network fail over time. A TCP application is not recovered until TCP has retransmitted lost data. TCP continuously adjusts its retransmit time after transmission delays and repeated network errors. Standard TCP has a minimum value for retransmission of one second. This means that even if network fail over occur instantly, application data is not recovered until one second has elapsed. The default value of the RNRP parameter **Send Period** has been set up to reflect this limitation.

Node Down Notification

A single lost message does not cause a Node down event. The time until a Node down event is generated is configured by the parameter **MaxLostMessages** (see [Table 5](#) on [page 55](#)).

Time until node down event = (**MaxLostMessages** + 1) * SourceSendPeriod
(normally (3+1)*1=4s).

Multiple Network Areas and RNRP Routers

There are a number of reasons why a network should be divided into Network Areas (subnetworks):

- Fault isolation. An erroneous network segment (bad cable, Ethernet switch or interface card) can not affect nodes on an other Network Areas.
- Traffic filtering. Undesired traffic can be blocked by a router if filter software is installed. This is true for a Windows Server node.
- Limitation of broadcast traffic. A router does normally not forward broadcast and multicast messages.
- The network is distributed over large distances using link protocols with different network characteristics. PPP is one example.
- The IP routing resources (Routing table, ARP table or CPU power etc.) in a single node are not large enough to handle a large number of nodes on the same Network Area.

For best performance the network designer should try to keep the time-critical traffic within the same Network Area. The time to change router node is always greater than the time to change path within the Network Area.

The Network Areas are interconnected by RNRP routers. A node with RNRP and connections to more than one network area can act as an RNRP router. In a PC additionally the flag “Enable TCP/IP forwarding” has to be set to 1 (see [Table 5](#) on page [55](#)).

Limit the number of hops

A message between two nodes can be forwarded via several network areas. The number of routers it goes through is described by the term “hop count”. Network topologies with many hops must normally be avoided. The reason is that a large hop count increases the probability for undesired behavior such as routing loops and slow response time due to delayed updates from distant routers. The default max number of hops is 3. The maximum value is 5.

Limit the number of network areas

An RNRP network can consist of 36 network areas. Windows nodes can handle up to 36 network areas but Controllers can only handle up to 15 remote areas that are reached via routers, in addition to the areas (1 or 2) that the controller are directly connected to. A node for which the “max number of remote areas” is exceeded will not get routing entries for all network areas. This means that it will be unable to communicate with some nodes on the network, and it can not be predicted which nodes this is. To avoid this problem it must be made sure that, for all nodes the number of network areas that are within “max number of hops” does not exceed “max number of remote areas”.

Connectivity Servers as Routers

In systems where the Control Network and the Client Server network are separated, the network is built up by different network areas. The connectivity servers that are connected to both networks, as in [Figure 8](#), will work as RNRP routers provided that IP forwarding is enabled (see above). This makes it possible for all nodes on the Client Server network to communicate with all the Controllers on the Control Network. This is used by the Control Builder in an Engineering Client when it

communicates with the Controllers. The routing through the Connectivity Servers is also needed for the network alarm handling to work properly, see [Node Status Alarms](#) on page 236.



The function “Show Remote Systems” in the Control Builder and the OPC server uses broadcasting and does therefore not work through routers. The IP addresses of the controllers have to be known and entered manually when the networks are separated.

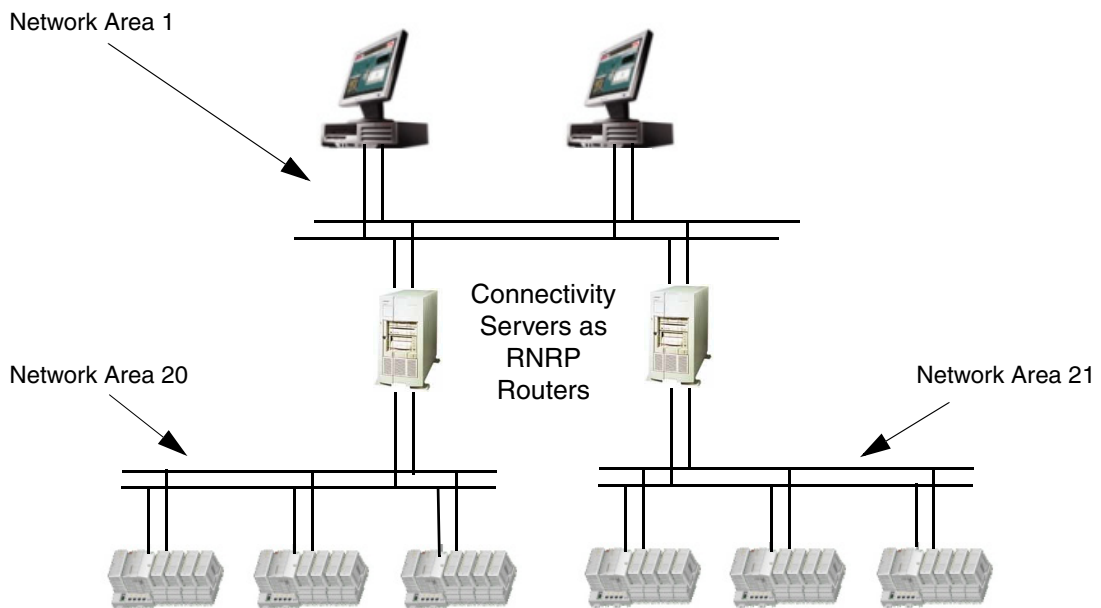


Figure 8. Network with Three Network Areas and Connectivity Servers as Routers

Controllers as Routers

The AC 800M controller can be used as router between non-redundant networks. There is no parameter to enable the routing capability. It is always enabled when RNRP is used and the controller is connected to two different network areas.



It is not possible to use two AC 800M Controllers to achieve a redundant connection between two redundant networks. For this 4 network interfaces per router is needed. This is described in [Figure 10](#) on page 46.

Redundant Connectivity Servers/Routers

A Connectivity Server (router node) can be a single point of failure. The RNRP protocol allows redundant router nodes between Network Areas. In the configuration below RNRP selects the router with lowest node number as the active router node. If this node fails the RNRP protocol selects the other router as active.

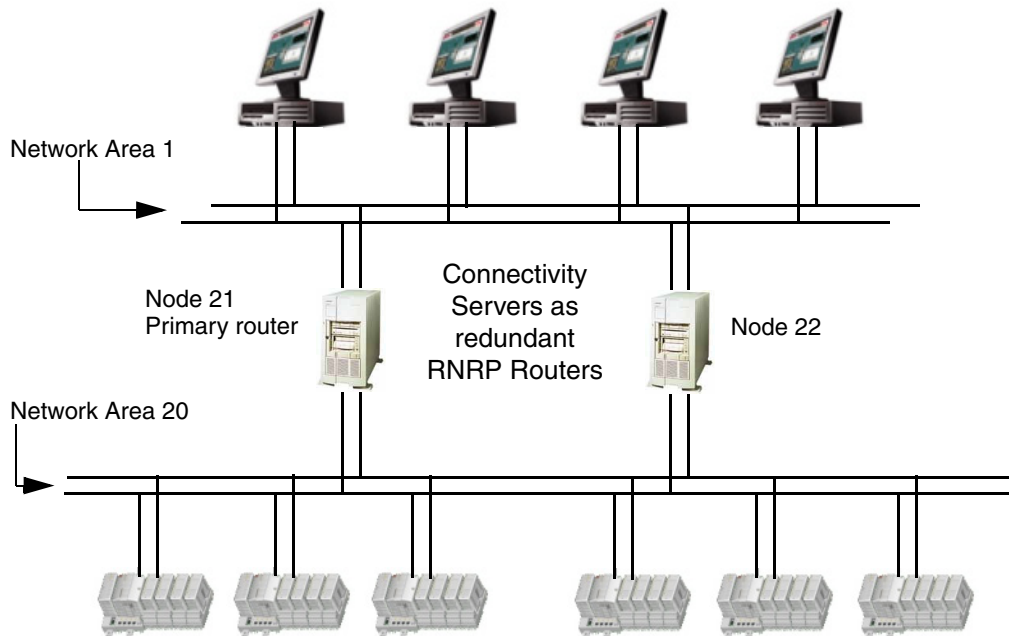


Figure 9. Two Network Areas with Redundant Connectivity Servers as Routers

In cases where multiple routes exist to a remote Network Area, **the router that has the highest number of reachable nodes** is selected as primary. If all routers have an equal number of reachable nodes then the **router with the shortest distance (hop count)** is selected as primary. If routers have equal distance then the intermediate **network with lowest Network Area number is selected as the primary**.

The network engineer should recognize that if serial links are used within the Control Network, throughput will be very low as compared to Ethernet alone.

In mixed configurations, it is recommended to put low Network Area numbers on the high capacity networks and high numbers on slow networks.



A good rule to follow during network configuration is to make sure that all alternative routes to destination nodes have equal distance (hop count). A network error should not cause redirection to a route with a greater distance. By following this rule, a network error will not change the node-to-node response time and no node will receive unpredictable loads from transit traffic.



An RNRP router has several advantages compared to a standard IP router:

- No manual routing configuration is needed.
The routing information about all nodes and networks is spread automatically.
- The routers can be redundant.
It is not possible to avoid a single point of failure when connecting two redundant RNRP network areas with a pair of standard IP routers. To do this two RNRP routers with 4 network ports each are needed, see [Figure 9](#) on page 44 and [Figure 10](#) on page 46. Such a router can only be built using a PC with 4 network interfaces. It is not possible to achieve the same functionality with two routers with two ports each.

Default Gateway Routing for Nodes without RNRP

If nodes that do not support RNRP are connected to the control network, e.g. managed switches or time servers, and these nodes need to be accessed (by nodes that use RNRP) via the RNRP routers the necessary routing information can not be built up by RNRP. One way to solve this is to enter the primary Control Network address of the primary connectivity server as “Default Gateway” in these nodes to inform them about how to reach the Client Server network.

Routing between Control Networks

Controllers on Control Network areas can communicate with each other if the Connectivity servers work as routers as in [Figure 8](#) on page 43. If it is desired that controller-to-controller communication is independent from the operation of the Connectivity servers and/or from the Client Server network it is possible to build a network where control networks are directly connected via dedicated routers.

Figure 10 shows two control network areas that are connected via a redundant pair of dedicated routers.

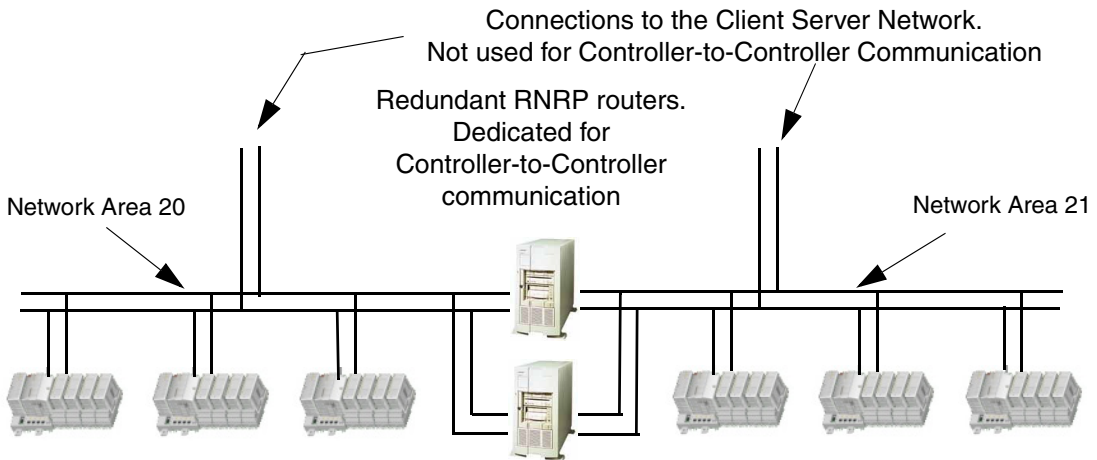


Figure 10. Redundant RNRP routers for Controller-to-Controller communication

Special Routing Consideration

A message can only be received on the Network Area on which the message's destination address belongs. Even if the message destination node is connected to multiple Network Areas and an alternative route exists through one of these other Network Areas, the protocol will not reroute to reach the destination node if the first Network Area breaks down.

Figure 11 on page 47 shows an example with an application in node 71 that has a session to target node 22 in Network Area 1. If node 22 loses both paths (double fault) on Network Area 1, then the application will lose the current connection even if it in theory is possible to route via Node 21 to Node 22 on Area 20.

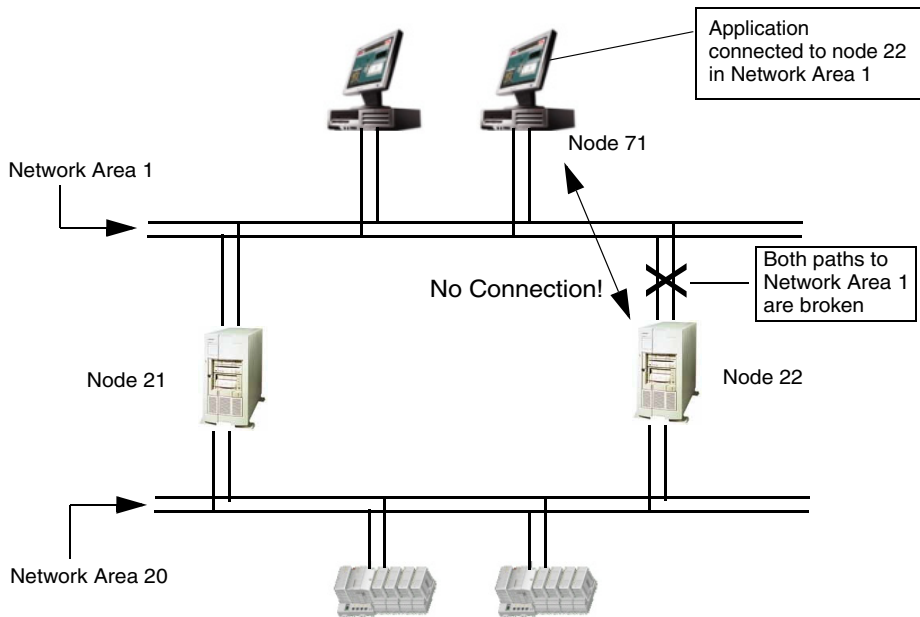


Figure 11. A Network Connection is lost if all Paths to a Node in the Destination Network Area are Down

Local Network Areas

The RNRP protocol permits Network Areas to be declared as “Local”. A Local Network Area does not distribute information about own networks and nodes to adjacent Network Areas. Traffic from other Network Areas can not be routed over this local Network Area. Only nodes directly connected to a Local Network Area can use it. In this way, nodes within the Control Network can use dedicated networks without risking being overloaded by transit traffic.

Building large networks by using Backbone Network Areas

RNRP normally gives both redundancy and supervision between all nodes in the whole network. These features lead to some of the size restrictions for an RNRP network, for example the number of network areas.

If node to node supervision (fast detecting node up/node down) is not necessary between nodes in all different areas it is possible to build a large network by using a “Backbone Network Area” to interconnect up to 35 Network Areas.

A Backbone Network Area is similar to the Local Area with the difference that routing information can be received from neighbor areas but no routing information is sent out to standard neighbor areas. A node connected in the Backbone area receives all network information from all network areas (except local areas). A node in a standard Network Area does not get any network information about nodes and networks in the Backbone Area or other Network Areas. This means that those network areas do not occupy any network resources in the nodes in the standard network areas so when deciding the values for the parameters Number of remote network areas and Max number of hops (see Table 5 on page 55) the Backbone Network Areas and areas beyond these do not need to be considered.

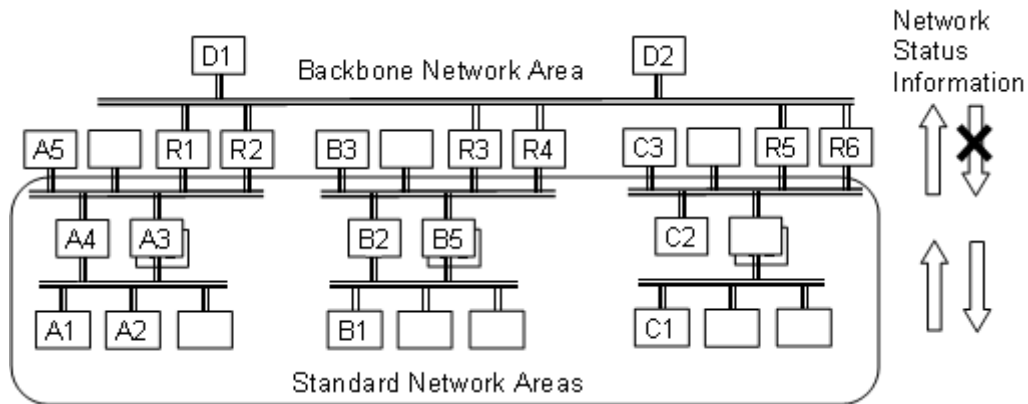


Figure 12. Using a Backbone area

In Figure 12 the function of the Backbone area means that (not all relations are mentioned):

- A nodes get supervision information about each other.
- B nodes get supervision information about each other.
- D nodes get supervision information about A, B and C nodes
- A and B nodes do not get supervision information about C and D-nodes
- Communication between A, B and C nodes is possible via Default Gateway (non redundant) or via External Network Service (redundant), see below.

Routing to or via a Backbone Area

Nodes in a Standard Network Area that need to communicate with nodes in a Backbone Area or an area beyond the Backbone area can configure the RNRP router connected to the Backbone area to be their Default Gateway.

If this communication needs to be redundant the parameters for External Network Service (see [Table 5](#) on [page 55](#)) shall be used to refer to the router connected to the Backbone area. Use the primary address of one of the routers and the secondary address of the other router.

Example of setup required for nodes on Standard Network Areas in [Figure 12](#) to communicate with A, B, C, D over Backbone Network Area.

If the routers R1 and R2 have the addresses 172.16.4.23 and 172.16.4.24 on the Standard Network area (down side interfaces) then these are the addresses to enter as the Router 1 and 2 addr to External Network in A-Nodes(A3/A4/A5) having direct connection to R1 and R2. A-Nodes below A3 and A4 sets Router 1 and 2 with addresses to A3 and A4.

If R3 and R4 have the addresses 172.16.8.23 and 172.16.8.24 on the Standard Network area then these are the addresses to enter as the Router 1 and 2 addr to External Network in B-Nodes having direct connection to R3 and R4. Other B-Nodes below B2 and B5 like B1 sets Router 1 and 2 with addresses to B2 and B5.

The parameters Number of remote network areas and Max number of hops can be left at the default values for all A, B and C nodes. This is because these nodes will not receive any network status information about the nodes in the network areas beyond the backbone area and therefore no resources will be required for them. For nodes directly connected to the Backbone area these parameters need to be configured considering all network areas. In this example all D and R nodes need to use Number of remote network areas ≥ 6 and Max number of hops ≥ 2 .

The parameters External Netw and External Netw addr mask can be used to filter the routing through the back bone area. This is a kind of security measure: only messages to addresses that match the External Netw and External Netw addr mask will be sent to the External Network Router. If for example all network areas in the network use a network ID starting with 172.16 it is recommended to set External Netw to 172.16 and External Netw addr mask to 255.254.0.0. With these settings the External Network Service Routers will be used for all messages to nodes with valid addresses inside the system network, but they will not be used for messages to

other nodes. If there is a request message coming from another external address, e.g. from an intruder node, the node that got the request will not use the External Network Service routers and does therefore not know where to send the responses, so it can avoid responding to some intrusion attempts.

RNRP Address Configuration: Implicit or Explicit



It is strongly recommended that the addresses presented in, [Recommended IP Address Plan](#) on page 30, are used. If they are used, no extra RNRP configuration is required and the following chapters about addressing may be ignored.

A node on a TCP/IP network is identified by its 32 bit IP address. The IP address¹ consists of a NetID part and a HostID part. The subnet mask specifies the boundary between the NetID and the HostID.

A node with more than one network interface must have a unique IP address for each interface.

Since RNRP is based on IP routing this is also true for all nodes running RNRP.

The interfaces in a node running RNRP are, in addition to the IP address and the subnet mask, also configured with the following logical address parameters:

- Network Area 0 - 31
- Local Flag 0 = Normal Network Area
 1 = Local Network Area, no routing to this area.
 This area is not announced to other areas.
- Node Number 1 - 500
- Path Number 0 - 1

The only mandatory rules for these parameters are:

- The Node number must be the same as the HostID (the least significant, right most bits in the IP address).
- For all nodes in one system the NetID (the most significant, left most bits in the IP address) must uniquely correspond to one Path in one Network Area. This means that:

1. IP addresses are described in more detail in the Appendix, section [IP Addresses](#) on page 247.

- All interfaces (in all nodes) on the same path in one Network Area must use the same NetID, i.e. be on the same subnet. This is as for all IP based communication, else they cannot reach each other.
- For interfaces with different NetID either the Path or the Network Area must differ.

To simplify the configuration of the network interfaces there is a set of additional rules.

If these rules are also followed, the RNRP address parameters are automatically configured. This is called the Implicit RNRP Configuration Method. See [Address Rules for Implicit RNRP Configuration](#) on page 52.

If only the mandatory rules are followed, the RNRP address parameters have to be configured manually for each network interface. This is called the Explicit RNRP Configuration Method.



Some more details about how to select IP addresses can be found in Appendix A [How to Choose IP Addresses](#) on page 249.

Using Explicit RNRP Configuration

Examples of how to apply the mandatory rules for explicit RNRP configuration:

If somebody decides that his/her system needs to use the subnet mask 255.255.0.0 the 3rd digit can not be arbitrarily chosen. For example the node address 10.11.12.13 can not be used because the HostID is $12 * 256 + 13 = 3085$, HostID must be the same as the node number and the node numbers can only be 1-500. The allowed addresses with this subnet mask are x.y.0.1 - x.y.1.244. The address x.y.1.200 is used on the node with node number $256 + 200 = 456$.

If somebody decides that his/her system only is allowed to use two different subnets this means that this only can be a system with two non-redundant network areas or a system with one network area with network redundancy.

A system with two network areas with network redundancy uses 4 subnets, i.e. 4 NetIDs.

In a system with subnet mask 255.255.255.0 the two interfaces (in two different nodes) with addresses 10.11.12.13 and 10.11.12.243 shall be connected to the same network. They are on the same path on the same network area. 10.11.13.12 shall be

connected to a different network. It is either on a different path or on a different network area. If the path or the network area or both differ depends on the settings of the parameters for path and network area in the different nodes.

First Project download when using other addresses than 172.16.x.x



If implicit RNRP configuration with Default Network ID=172.16.0.0 is not used (i.e. when using explicit RNRP Configuration and also when using implicit RNRP configuration with Default network ID different from 172.16.0.0) the first project download to an AC 800M Controller must be done from a Control Builder running in a PC which is connected to the Control Network, i.e. with no router between the PC and the Controller. This means that it for example can not be done from an Engineering Client which is only connected to the Client Server network. It can be done via PPP on COM4.

This is because RNRP needs to be configured for the routing to work and the only way to set the RNRP parameters is by downloading a Control Builder project to it. This first project may be a project which only contains the HW configuration for the Processor Module with the correct RNRP parameters. That project can later be replaced with the project which is engineered with the real application.

Address Rules for Implicit RNRP Configuration

With the implicit RNRP configuration method all IP addresses have a strict relationship to the RNRP address parameters so that the RNRP address parameters can be encoded within the configured IP address. This means that it is sufficient to configure only the IP address. RNRP can calculate the other address parameters from the IP address. This is done in each node. The easiest method is to just use the addresses according to [Table 2](#), [Table 3](#) or [Table 4](#). It is however possible to use other addresses by following these steps:

1. Choose the RNRP address parameters
2. Choose the Base Address.

The base part of the IP addresses: $N_1.N_2.0.0$

(N_2 must be a multiple of 4, i.e. $N_2=4*n$ where $n=0$ to 31)

This may be chosen freely from RNRP's point of view, but they must be the same in the whole system. Using the default 172.16 reduces the configuration work.

3. Calculate the IP address based on the RNRP address parameters as shown on [page 53](#).
4. Set subnet mask to 255.255.252.0

When using implicit configuration the address mask must be set to 255.255.252.0. This gives 10 bits for the HostId, i.e. 1024 addresses. This allows the HostID to be identical to the RNRP Node number that can be 1-500 for normal nodes and 513-1013 for backup CPUs in Redundant Controllers (see [Mixing Explicit and Implicit RNRP Configuration](#) on page 61).

Below there are two ways of describing how to calculate the IP address based on the RNRP address parameters. They give the same result but one or the other may be simpler to use in different situations.

Calculating the IP Address Bit by Bit

With a binary representation the IP address must be created as:

XXXXXXXXX.XXXXXXPP.LAAAAANN.NNNNNNNN

where the bits are:

XXXXXXXXX.XXXXXX	XXXXXXXXX.XXXXXX00.00000000.00000000 is equal to the Base Address The 14 first bits is the Network Identity
PP	Path Number
L	Local Flag
AAAAA	Network Area Number
NN.NNNNNNNN	Node Number

Calculating the IP Address Byte by Byte

With a byte wise representation the IP address must be created as: A.B.C.D

where the bytes are:

$$A = N_1$$

$$B = N_2 + \text{Path}$$

$$C = \text{Local} * 128 + \text{Area} * 4 + \text{Node DIV } 256$$

$$D = \text{Node MOD } 256$$

$N_1.N_2$ is the Network Identity. Path, Local, Area and Node are the other RNRP address parameters.

DIV means an integer division and MOD means the Modulo operation, i.e. the rest after the integer division.

If the Local flag is 0 and the node number is less than 256 the formula is a bit simpler:

$$A = N_1$$

$$B = N_2 + \text{Path}$$

$$C = \text{Area} * 4$$

$$D = \text{Node}$$

Example:

Base Address = 172.16.0.0, Network Area = 2, Node number = 201
(Local = 0, Node number < 256) =>

Primary Network Interface (Path = 0): 172.(16+0).(2*4).201 = 172.16.8.201

Secondary Network Interface (Path = 1) 172.(16+1).(2*4).201 = 172.17.8.201

RNRP Configuration Parameters

RNRP has two groups of configuration parameters. One group contains base parameters that are common to all network interfaces in a node and another group contains parameters that may be specified for each individual network interface.

[Table 5](#) and [Table 6](#) below describe the parameters. The same parameters exist in a PC and in the Control Builder configuration but in some cases the names differ slightly. In these cases the table indicates where the names apply by (PC) and (Ctrl).



For most installations the default values for the RNRP configuration parameters are sufficient. This means that none of the parameters in [Table 5](#) and [Table 6](#) need to be modified.

If explicit RNRP configuration is used at least some of the parameters need to be set to other than the default values.

For a controller the RNRP parameters are set in the hardware tree in the controller project built in the Control Builder. The Base parameters are set on the hardware unit for the Controller CPU, e.g. PM860/TP860 and the explicit RNRP parameters are set on the hardware unit for the Ethernet interfaces and the PPP protocol definition on a COM-port.

In a PC the RNRP parameters are set with the RNRP configuration wizard, see [Configuring RNRP in a PC](#) on page 69. The base parameters and the explicit parameters are located under different tabs.

Table 5. RNRP Base Parameters

RNRP Base Parameters		
Parameter	Range	Description
Max number of own network areas (PC) RNRP Number of own areas (Ctrl)	1 - 8(PC) 1-4(Ctrl)	Maximum number of Network Areas that this node is directly connected to. An end node always uses one Network Area. A router has 2 or more own network areas. Default: 3(PC), 2(Ctrl), rarely changed
Max number of remote network areas (PC) RNRP Number of remote areas (Ctrl)	0 - 35(PC) 0 - 15(Ctrl)	Maximum number of remote Network Areas that this node can communicate with via routers. Default: 5(PC), 4(Ctrl), rarely changed
Base Address (implicit addresses) (PC) RNRP Default Network ID (Ctrl)	A.B.0.0	The network base address used at implicit RNRP configuration. Default: 172.16.0.0
Send Period (PC) RNRP Send Period (Ctrl)	1..60	The time period for multicasting of routing messages. This is also the minimum time for fail over in a redundant network. Range value in second units. Default: 1 Also read Network Fail Over Time on page 40.

Table 5. RNRP Base Parameters (Continued)

RNRP Base Parameters		
Parameter	Range	Description
Max number of lost messages (PC) RNRP Max Lost Messages (Ctrl)	1..10	Number of routing messages that may be lost until a path to a node is down. Time(s) to detect node down = Send Period * (Max Lost Messages + 1) Default: 3, rarely changed
Max number of hops (PC) RNRP Max no of hops Ctrl)	1..5	The maximum accepted hop count (number of passed routers) in the network. Default: 3, rarely changed
Number of explicit addresses (not configured in a controller)	0..8	Number of explicit specified network interface addresses with RNRP parameters. Default: 0. For a controller this is decided by the values of the RNRP address parameters for the Ethernet ports
Enable ICMP Redirects (not configured in a controller)	0..1	Windows' standard function for Internet Control Message Protocol redirects. It shall be disabled because it may destroy the routing table that RNRP maintains. Default: 0, do never change (Standard Windows Registry parameter. Visible as RNRP parameter just to make it easy to verify its value)
Disable Media Sensing (not configured in a controller)	0..1	Windows' standard function for Ethernet Media sensing. It shall be disabled because it may destroy the routing table that RNRP maintains. Default: 1, do never change (Standard Windows Registry parameter. Visible as RNRP parameter just to make it easy to verify its value)

Table 5. RNRP Base Parameters (Continued)

RNRP Base Parameters		
Parameter	Range	Description
Enable TCP/IP Forwarding (PC) (always enabled in a controller)	0..1	A flag that if set enables this node to be a router. It shall typically be set to 1 in a Connectivity Server. Default: 0 This is a standard Windows function. To make a change of this parameter effective the node needs to be restarted.
External Netw (PC) RNRP Ext network (Ctrl)	A.B.C.D	The IP address of the external network. Set 0.0.0.0 to use Router 1 and 2 as Default gateways without filtering. (See Routing to or via a Backbone Area on page 49 for example usage)
External Netw addr mask (PC) Ext netw mask (Ctrl)	A.B.C.D	The IP address mask of the external network. Undefined in case of Default Gateway
Router 1 to External Netw (PC) RNRP Ext router1 addr (Ctrl)	A.B.C.D	IP address to router 1 for the external network.
Router 2 to External Netw (PC) RNRP Ext router2 addr (Ctrl)	A.B.C.D	IP address to router 2 for the external network.

Table 5. RNRP Base Parameters (Continued)

RNRP Base Parameters		
Parameter	Range	Description
System type (PC) (fixed set in a controller)	1..127	System type that will be displayed by e.g. the RNRP Network Monitor. Note that bit zero is reserved and is not a part of the System Type. 1-70: Controllers 71-127: Workplaces
Enable Hosts file update (not configured in a controller)	0..1	Enables RNRP to update Windows hosts file. Default: 1 Setting it to 0 should normally never be done. Could be used for fault tracing of name resolution problems.



If the parameters, Network Identity, Send Period, and Max number of lost messages, are valid for all the network interfaces used in this node, no explicit interface parameters have to be defined and the value of parameter numExplicit must be zero.

If the base parameters are not acceptable to all Network Areas or if the implicit addressing scheme does not fit the installed network (true for all point-to-point links), then the RNRP parameters have to be specified explicitly for every individual network interface. Please see [Table 6](#).

For many parameters in the explicit tabs in the RNRP Wizard (see [Configuring RNRP in a PC](#) on page 69) and on the individual Ethernet interface for a controller setting the value 0 means that the corresponding base parameter will be used.

Table 6. RNRP Explicit Parameters

Parameters that may be specified for each Network Interface		
Parameter	Range	Description
IP address	A.B.C.D	The interface IP address. If point-to-point link, please read next chapter.
IP subnet mask	X.Y.Z.W	The IP address mask used on this interface. Normal value 255.255.252.0
Network Area	0..31 32..35	Network Area number on this interface. Tunnel Network Area numbers. Set to 0 if implicit configuration is used.
Network Area Local	0..2	1 = Local Network Area. 2 = Backbone area. Normal value is 0. Set to 0 if implicit configuration is used.
Path Number	0..1	Network Path number on this interface. Set to 0 if implicit configuration is used.
Node Number	1..500	The own Node number in this Network Area Set to 0 if implicit configuration is used.

Table 6. RNRP Explicit Parameters (Continued)

Parameters that may be specified for each Network Interface		
Parameter	Range	Description
Send Period	1..60	Routing update period. Range value in second units. Normal value is 1. 0 means use the corresponding base parameter.
Max Lost Messages (Ctrl) Max number of lost messages (PC)	1..10	Number of routing messages that may be lost until a path to a node is down. Normal value is 3. Time(s) to detect node down = receivedSendPeriod* (maxLostMessages+1) 0 means use the corresponding base parameter.
Remote IP address (Ctrl, Set on the HW unit for PPP) Point-to-point destination node (PC)	0..500	The peer node number. If specified, the protocol uses unicast instead of multicast/broadcasting. Only used for point-to-point links. Set to zero otherwise.
Proxy router	A.B.C.D	The IP address to a router not running RNRP that is used in a Tunnel Network Area. Only Network Areas 32 to 35 are defined as Tunnel Areas. Only used for Tunnel Areas. Set to zero otherwise.
Target addr	A.B.C.D	The IP address to the node on the other end of the Tunnel Area that belongs to a real Network Area. Only used for Tunnel Areas. Set to zero otherwise.



In a PC RNRP needs to be restarted to make a change effective of any of the parameters in [Table 6](#). This is done with the button “Restart RNRP”, see [Figure 18](#) on [page 71](#). In a controller a change of most of the parameters in [Table 6](#) will be effective without restarting RNRP.

If however the IP address or the IP subnet mask is changed the controller needs to be restarted to make the change effective.

Any controller restart works (short or long init or power fail restart), but the application restart at download is not enough.

A user that configures with explicit parameters must follow these rules:

- The Node number must be the same as the HostID (the least significant bits in the IP address). An exception to this rule is when the IP address mask is equal to 255.255.255.255 in which case RNRP will use the IP class C address internally, i.e. the Node Number must be equal to the least significant byte in the IP address, i.e. D if the IP address is A.B.C.D.
- Parameters nodeNo, sendPeriod, and maxLostMessages, must have the same values on both redundant paths within one Network Area.

Mixing Explicit and Implicit RNRP Configuration

All nodes on the same network area must use the same configuration method for the interfaces towards that area.

In different Network areas of a system it is possible to use different methods.

A node with connections to more than one network area can use different methods towards different areas. For a PC this means that the parameter Number of explicit addresses (see [RNRP Address Configuration: Implicit or Explicit](#) on page 50) will be > 1 but less than the number of network interfaces. For a controller this corresponds to setting Node Number, Network or Path number > 0.

Interconnection of Network Areas over WAN

System communications sometimes needs to use external network providers to cover sites distributed over large areas. This chapter only briefly describes different methods to interconnect Network Areas over WAN by different network services. Details about configurations, security and performance must be made up together with a selected network provider.

Shown possibilities are:

- Use of standard IP Routers
- Use of Layer 2 VPN or VLAN Tunneling
- Use of Layer 3 VPN

The first section covers routing and redundancy issues. The two following also cover security aspects of extending the system network.

Interconnecting RNRP Network Areas via Standard IP Routers

It is possible to connect RNRP Network Areas using standard IP routers and/or firewalls that do not run the RNRP protocol. This is done by configuration of RNRP Tunnel Areas. A Tunnel Area is a specification of IP routes and addresses in a path between two Network Areas. Both static network routes in the routers and explicit addresses to the routers in the Area border nodes have to be configured. See example below.

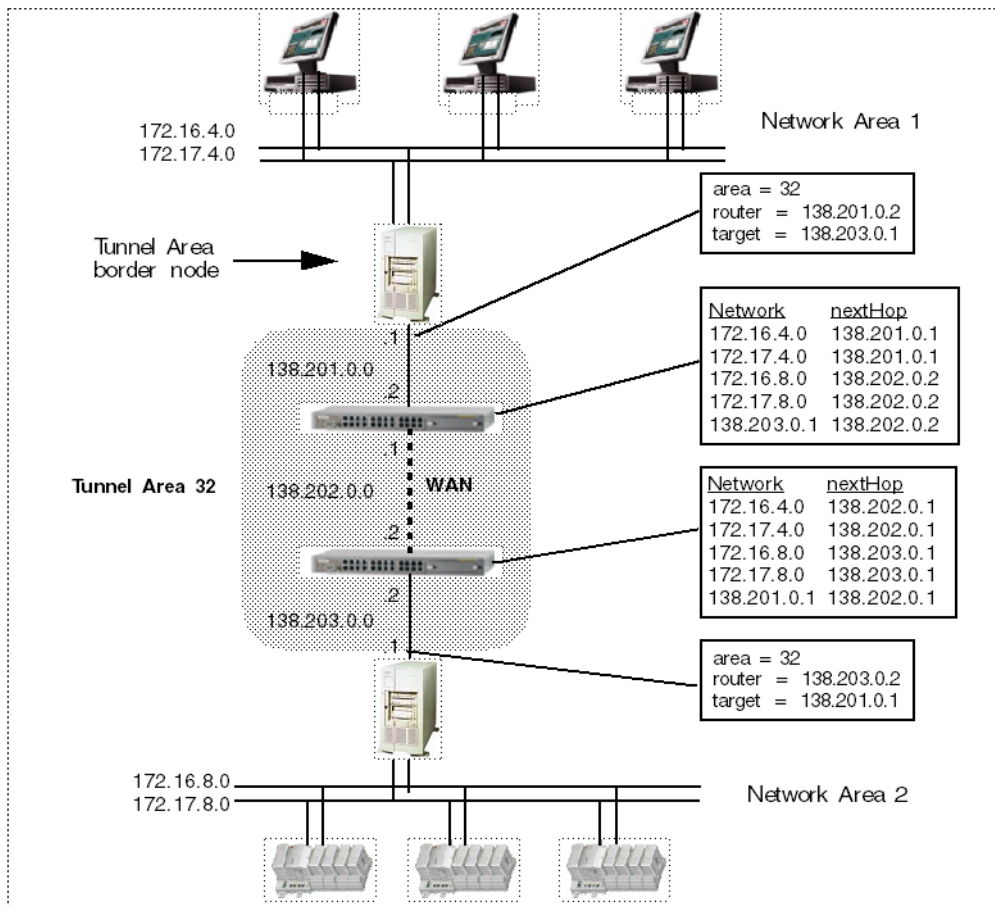


Figure 13. An RNRP Tunnel Area between Network Area 1 and 2

The network IP addresses inside a Network Tunnel Area can be freely selected, the RNRP protocol does not restrict IP address selection.

A Tunnel Area border node collects network information about all known Network Areas on its side of the tunnel and send the collected information to the Tunnel Area border node on opposite side of the tunnel.

An RNRP Tunnel Area only has one network path. There is no support of redundant paths within a Tunnel Area. If redundant connections are required then two parallel Network Tunnel Areas can be configured. This is shown in [Figure 14](#) on [page 64](#).

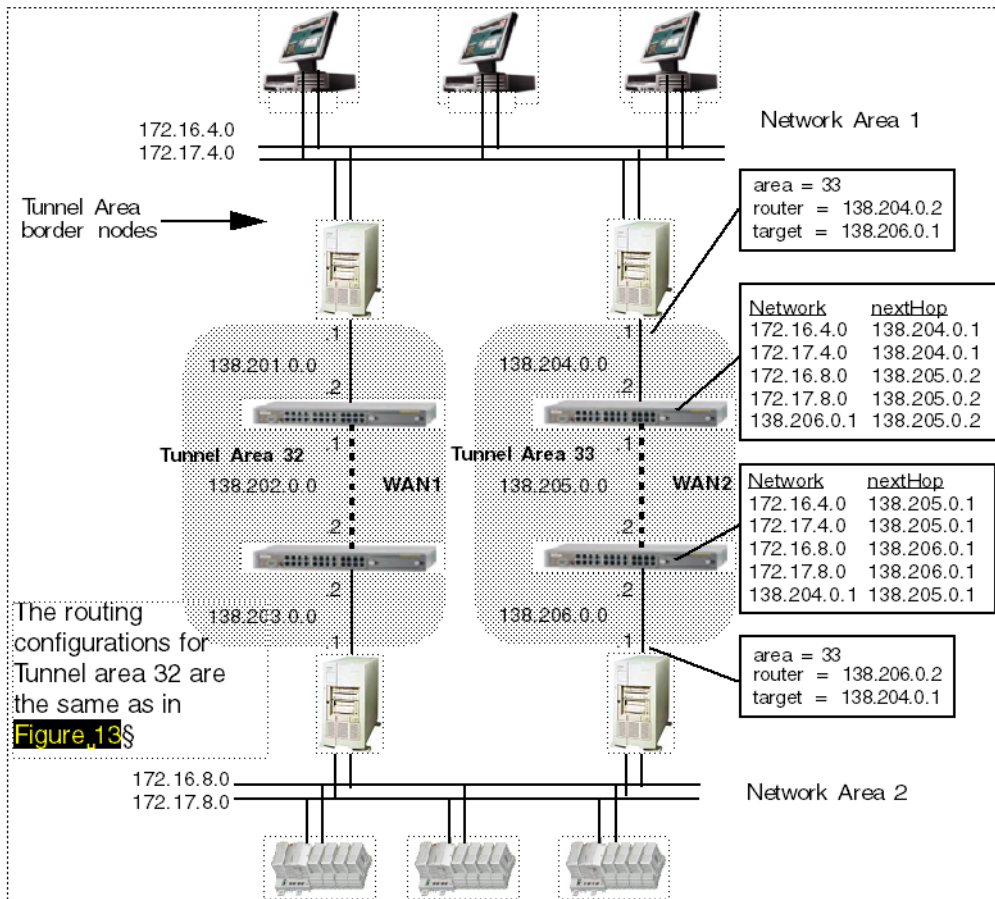


Figure 14. Redundant RNRP Tunnel Areas between Network Area 1 and 2

Applications inside the Tunnel Area border node itself do not get redundancy between the two Tunnel Areas. This means that the Tunnel Area border nodes should not be nodes that run applications that need to use the tunnel.

Do not use the Remote Access Server or the Remote Access Client (see [Multisystem Integration](#) on page 80) as Tunnel Area Border nodes if you want to use a redundant remote connection.

Figure 15 shows a system using Multisystem Integration with two tunnel areas. In this configuration the Remote Access Client has a redundant connection to the Remote Access Server.

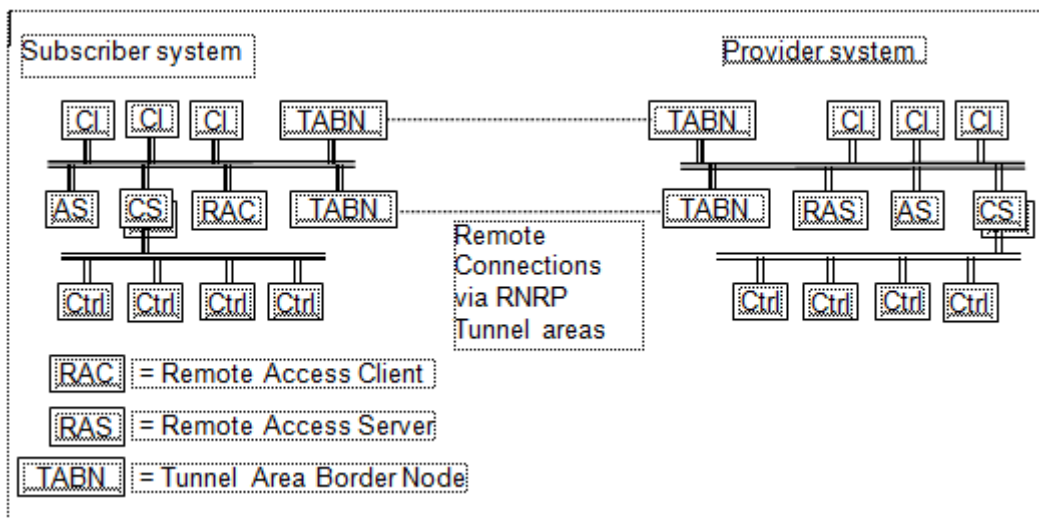


Figure 15. Multisystem Integration with Redundant Tunnel Areas

In the example above all nodes will have redundant connections to all other nodes (if also the connectivity servers are redundant). This might however not be desired. If the Remote Access Client and the Remote Access Server should be the only two nodes that communicate with each other IP filtering may be used in the tunnel area border nodes. If the remote connection does not need to be redundant this can be achieved by setting the tunnel area as a Local network area and to run the Remote Access Client and the Remote Access Server in the Tunnel Area Border nodes.

The Tunnel is not recommended to make direct use of public networks since the private Network Areas are exposed by the routers. If a link over Internet is requested than a secure tunnel using Layer 3 VPN technique is recommended. See [Use of](#)

[Layer 3 VPN Solutions](#) on page 67 and [Virtual Private Networks \(VPN\) for Secure Connections](#) on page 106.

Multisystem Integration is described in [Multisystem Integration](#) on page 80.

Use of Layer 2 VPN Solutions

A layer 2 solution enables the one and same RNRP Network Area to be distributed by use of VLAN and different network backbone technologies. For the clients point of view the network is transparent looking as single LANs. Clients and Controllers connect to VLAN ports on Ethernet devices. The traffic between the Ethernet devices are transferred by some type of routing or tunneling protocol. One possible protocol to use is Multi Protocol Label Switching (MPLS).

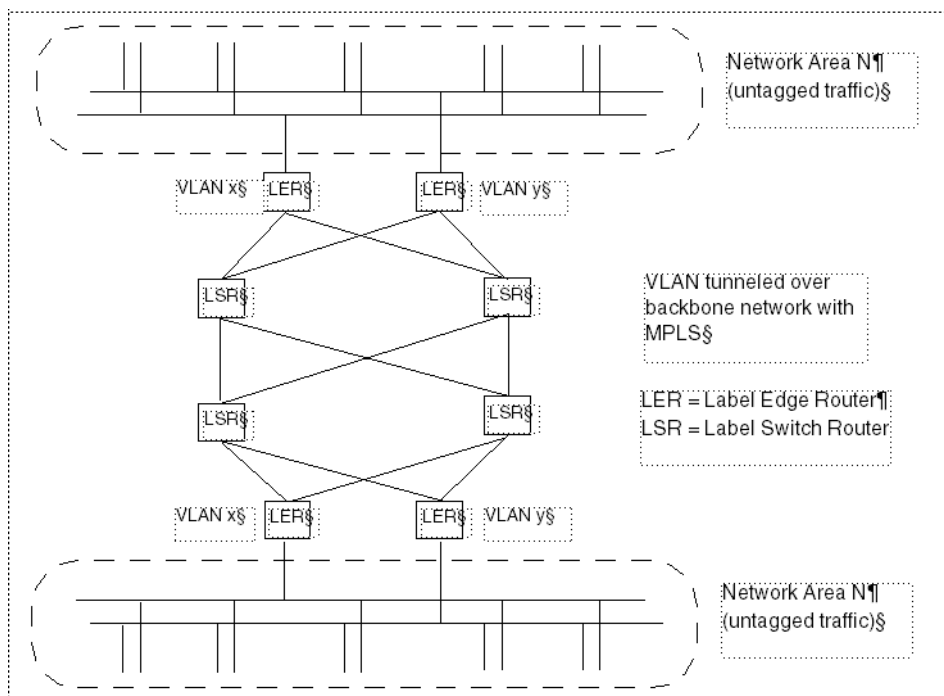


Figure 16. Layer 2 VPN, Example with MPLS Backbone

Use of VLAN makes RNRP configuration easy. The network transportation is invisible for RNRP. Both sides of the network belong to the same subnet and network area. See also [Reducing HW using Virtual LANs](#) on page 219.

Layer 2 VPN does generally not give the same security a Layer 3 VPN.

Use of Layer 3 VPN Solutions

Layer 3 solutions gives high security by using encrypted tunnels like for example the IPSec standard. Service providers has no visibility into IP tunnels. The traffic within a service provider can be routed as any other IP traffic.

The RNRP configurations is made in the same way as with RNRP Tunnels over standard routers, see [Interconnecting RNRP Network Areas via Standard IP Routers](#) on page 62.

The VPN tunnel must be able to tunnel data from nodes on different subnets on each remote site.

Layer 3 solutions are generally slower than Layer 2 solutions.

Microsoft Windows Server 2008 supports the two Layer 3 solutions PPTP and L2TP.

See also [Virtual Private Networks \(VPN\) for Secure Connections](#) on page 106 and [Site to Site Connections via a Firewall](#) on page 112.

RNRP in a PC

This section describes how to install and configure RNRP in a PC.

Configuring a Network Adapter

The manual *System 800xA Installation (3BSE034678*)* includes a description of how to configure the network adapter. The following parameters shall be configured:

- The IP address
See [Selecting IP Addresses](#) on page 29.
- The Subnet Mask
See [Selecting IP Addresses](#) on page 29.

- The DNS server addresses
See [DNS Configuration in Each Node](#) on page 132.
- If the interface shall be automatically registered in DNS
See [DNS Configuration in Each Node](#) on page 132..



After change of any network adapter property always check using the RNRP Monitor that nodes are reachable. Some adapter loses multicast addresses after configuration changes.

The problem can be repaired by doing the following:

1. Start the RNRP Monitor.
2. Disable the Network Adapter showing no nodes on the subnet.
3. Wait for a Netw_down event
4. Enable the Network Adapter.



A Network Adapter in a PC must never be permanently Disabled. If it is disabled the network redundancy function is lost.



If the Network Adapter has the multi core feature “**Receive Side Scaling**” this feature **must be disabled**. If this is not done duplicate network messages may be received and RNRP may interpret this as a “Suspected Network Loop”. See [RNRP Network Loop Detection and Protection](#) on page 72.

Installing RNRP

RNRP is installed together with other products.

It is always included in the AC 800M controller firmware.

For PCs it is automatically installed when 800xA Base is installed.

RNRP can also be used in PCs that do not use any other 800xA software.

On the 800xA System DVD RNRP is available as a component that can be installed without the rest of the 800xA System.

The recommended method to install RNRP on clients and servers is to let the System Installer do it. This is true also for the installation on the Domain Server.

Configuring RNRP in a PC

Normally the only item to configure is the IP address for each Network Adapter and this will be handled during the installation of Windows.



If the implicit RNRP configuration is used normally RNRP does not need to be configured after being installed.



It is possible to configure more than one IP address for a network interface in a PC. It is even possible to use that second address for a second RNRP network area. It is however not recommended to run two standard network areas on the same physical network unless VLANs are used (see [Reducing HW using Virtual LANs](#) on page 219).

To use a PC as a RNRP router (e.g. a connectivity server) the parameter **Enable TCP/IP Forwarding** must be set to 1. After this parameter is changed the node needs to be restarted.

Explicit RNRP configuration (and configuration of RNRP Base parameters e.g. TCP/IP Forwarding, see [RNRP Configuration Parameters](#) on page 54) in a PC is done with the RNRP Setup Wizard that can be found with a right-click on the RNRP icon in the System Tray or at **Start > All Programs > ABB Industrial IT 800xA > System > Network > RNRP Wizard**, see [Figure 17](#).

The RNRP icon is normally listed at **Start > All Programs > Startup** to be activated automatically when a user logs in. It can also be started by **Start > All Programs > ABB Industrial IT 800xA > System > Network > RNRP Create Icon**.

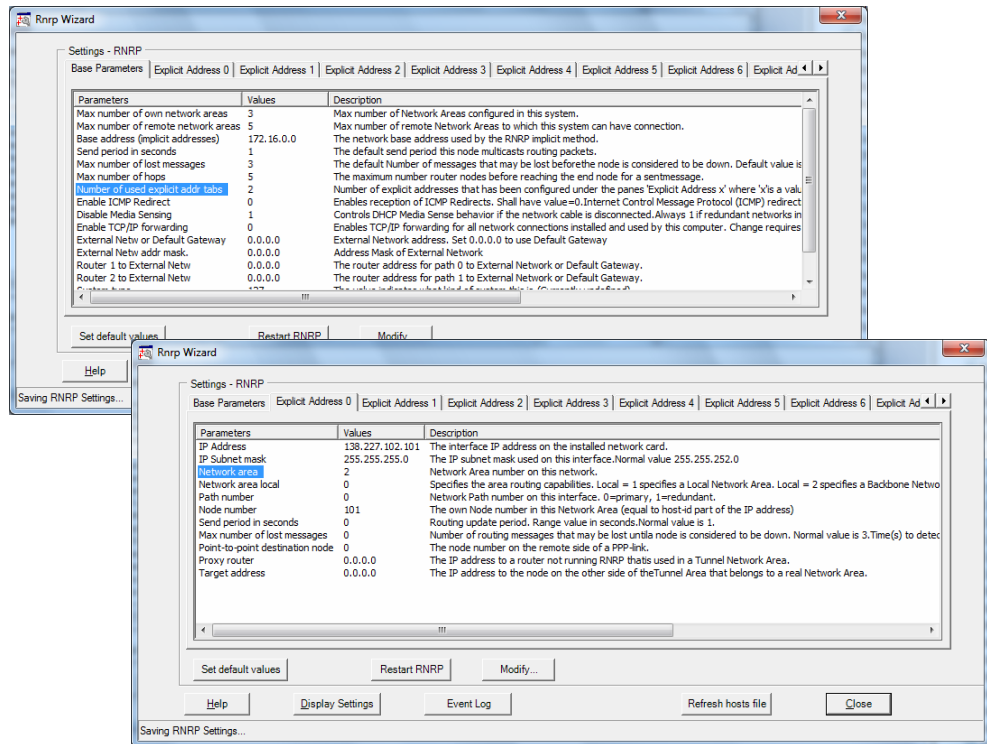


Figure 17. RNRP Setup Wizard Mainly for Explicit Configuration of RNRP, the Tabs “Base Parameters” and “Explicit address 0”

Verify RNRP Connectivity

Use the RNRP Network Event Monitor (see [RNRP Network Monitor](#) on page 237) to verify that the PC has contact with all other nodes that run RNRP.

Configuring what Networks to Use

In order for system communication applications in an 800xA System to follow the rule that all connections must be established using primary address (see [page 39](#)) the system needs to know what network areas and paths it should use.

The configuration is done at “Create System” (or later) with two dialogs.

One dialog where you first tell the number of network areas where 800xA PCs will communicate. This should be network areas where clients and servers communicate with each other. Network areas where only controllers and connectivity servers are connected do not need to be accounted for here. The number is 1 in almost all systems. After the first question you get the dialog shown in [Figure 18](#). Enter the network address information for the Client Server network.

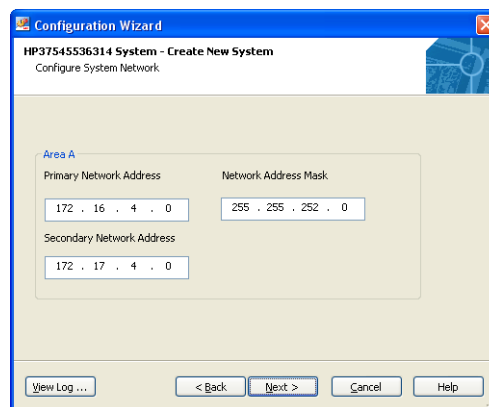


Figure 18. Dialog to Configure Network Areas where PPA Nodes Communicate



The configuration is intended for the 800xA System applications if a redundant Client Server network is used or if clients and/or servers are connected to a network in addition to the Client Server network. The purpose is to prevent the clients and servers from establishing connections on the wrong network.

RNRP Network Loop Detection and Protection

A misconfigured network with multiple paths may lead to a network loop. A network loop may cause a broadcast storm where the nodes in the network receive the same packets over and over again potentially causing a CPU overload which leads to a shut down of the AC 800M controller.

RNRP provide a function to detect network loops. If the same RNRP packet is received several times the event will be reported and an action taken.

In AC 800M a warning indication will be set in the Unit Status for the HW Unit **Ethernet**. The warning text is **Network Loop detected**. The warning can be seen in the Control Builder and in the System Status Viewer and it triggers a system alarm with High Priority.

In Windows RNRP will protect the system by disabling the port where loop is detected.

If redundant network is configured the traffic can continue on the other network.

In AC 800M the protection function is provided by the Network Storm Protection. Refer to [AC 800M Network Storm Protection](#) on page 121.

If the RNRP network loop protection has disabled a network:

A disabled port can be enabled via the RNRP Fault Tracer. The Fault Tracer can also be used to find which nodes that have detected a network loop. If the port is not enabled manually it will be automatically enabled 1 hour after it was disabled. If there is still a network loop on the network the port will be closed again.

Section 3 Distributed System Topologies

This section describes examples of how to build 800xA Systems where different parts of the system are located more or less far away from each other.

The standard system, where all nodes are located at more or less the same place, is described in [Figure 19](#) below..

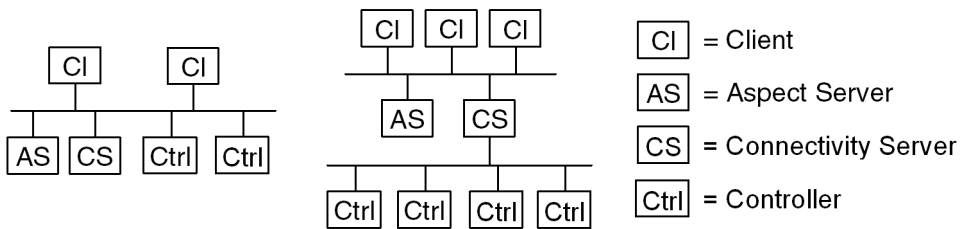


Figure 19. Standard System Topologies

For the discussion in this section there is no principle difference between the left system with combined client server and control network and the right system with separated networks.

The following sections describe different system configurations using remote connections.

The focus here is where to place different node types. [Section 5, Network Security](#) describes how to make sure that the remote connections are secure.

Extend the 800xA Automation System Network

A straight forward approach to building a system where some of the nodes are located far away is to simply extend the Automation System Network.

As long as the network equipment supports building an ethernet network with the same performance as on a local network there is nothing special to consider for an extended system network. The paragraph [Ethernet Speed](#) on page 215 describes performance considerations for the Automation system network.

If a controller is located far away, extend the Control Network to reach this place, see [Figure 20](#) below.

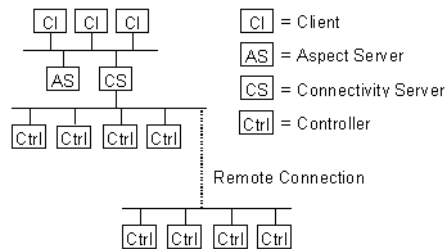


Figure 20. Remote Controllers on an extended Control Network

If a client or a server is located far away, extend the Client Server Network to reach to that place, see [Figure 21](#).

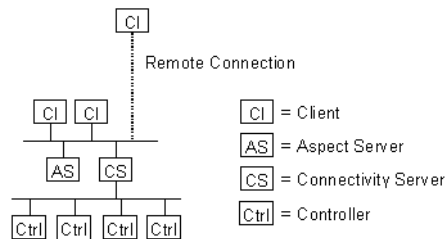


Figure 21. Remote Client on an extended Client Server Network

The traffic on the client server network normally is heavier than the traffic on the Control Network. This means that if all controllers are located far away, it is still recommended to locate the connectivity servers centrally and to extend the Control Network over the remote connection. See [Figure 22](#) and [Figure 23](#).

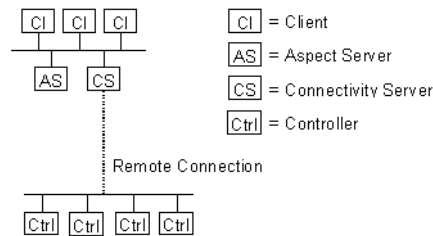


Figure 22. Locate Connectivity Servers centrally, extend the Control Network

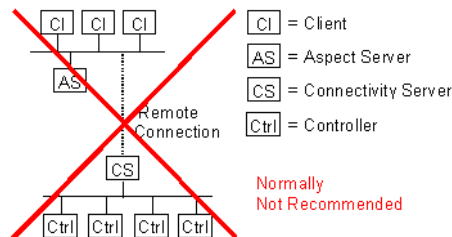


Figure 23. Avoid locating the Connectivity Servers together with the Controllers

If it is desired to have both client workplace functionality and controllers at a remote location the recommended solution is to place both connectivity servers and clients at the remote location¹, see [Figure 24](#).

It is not recommended to place only the controllers and the clients there as in [Figure 25](#). The reason is that this would mean that the remote connection needs to be used for both the Control Network and Client Server Network since the Workplace Clients do not communicate directly with the controllers. All OPC communication goes via the Connectivity Servers.

1. If the performance allows it the workplace may be run on the Connectivity Servers. Otherwise the workplaces should be run in separate client nodes.

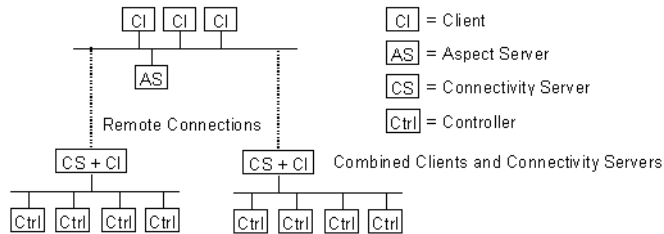


Figure 24. Remote combined Clients and Connectivity Servers

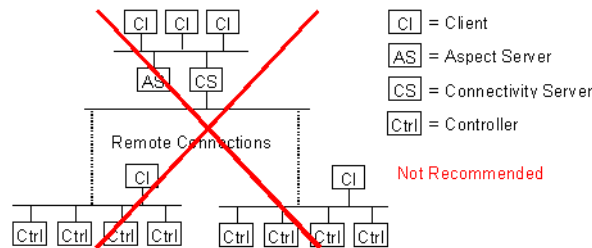


Figure 25. Do not connect Clients to the Control Network

If both the Client Server Network and the Control Network need to be extended the straight forward solution would be to build two remote connections (4 in case of redundancy). If the remote connection has sufficient bandwidth it is possible to run both networks on the same link. To separate the networks VLANs can be used as shown in figure [Figure 26](#). Section [Reducing HW using Virtual LANs](#) on page 219 describes more about how to do this.

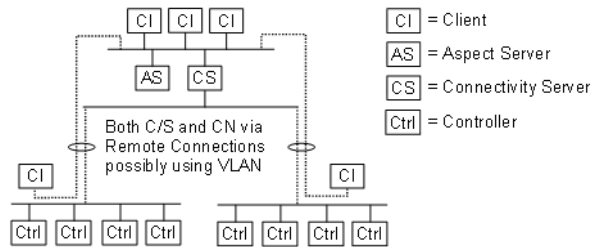


Figure 26. Clients close to the Controllers, extended Client/Server Network

If it is desired that the remote nodes can operate independent from the rest of the system, in case for example the remote connection is broken or if there is a problem with the central part of the system, the automation system may be designed using two or more 800xA Systems that are connected together using the function “Multisystem Integration”¹. Multisystem Integration is described in [Figure 27](#) and in further details in [Multisystem Integration](#) on page 80.

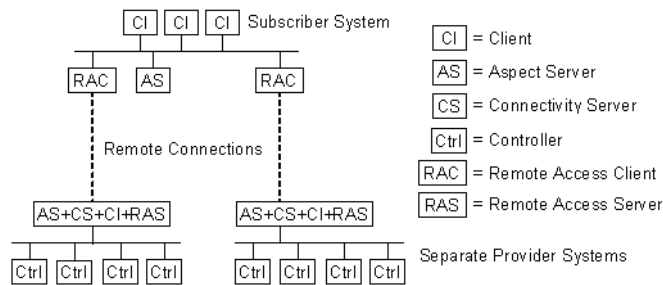


Figure 27. Remote separate 800xA Systems with Multisystem Integration

1. Depending on the system size the provider system may consist of one or several nodes

Equal System Sections on Different Locations

For some distributed systems the topology may not be described as one central location with most of the system and one or more remote locations, but rather as two or more locations that all are similar to each other with perhaps all node types on all places.

Also in such case it may be considered to build one distributed 800xA System with an extended Automation system Network. Which parts of the automation system network to extend depends on which type of data needs to be exchanged between the nodes on different locations.

If the controllers do not communicate time critical data directly between the two locations it is recommended to use separate Control Networks, one on each location, and to extend the Client Server network between the locations, see [Figure 28](#).

If controllers communicate much with each other between the two locations the control network may need to be extended, see [Figure 29](#).

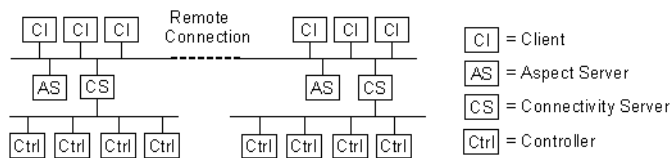


Figure 28. One 800xA System with two connected equal parts

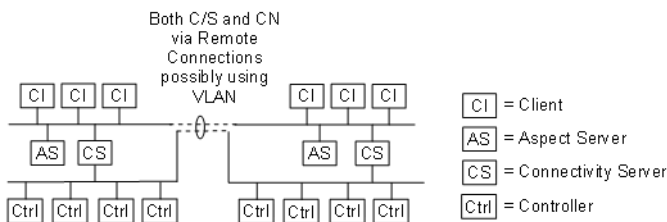


Figure 29. One 800xA System, Both Networks extended

For a distributed 800xA System to work with full functionality the remote connection needs to be reliable. If it is broken some functions may be lost. For example: In a system with 2oo3 redundancy for the Aspect Servers with two Aspect Servers on one side of the connection and one on the other, the side with only one Aspect Server can not be engineered if the remote connection is broken.

Building the distributed system as one 800xA System makes it possible to both operate and engineer the whole system from both locations. As mentioned previously a method to make two locations less dependant of the connection between them is to use the function Multisystem Integration, see [Figure 30](#).

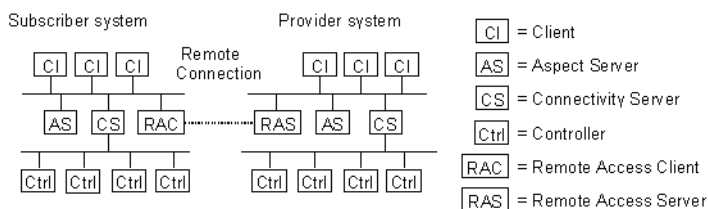


Figure 30. Two 800xA Systems connected using Multisystem Integration

With Multisystem integration one of the parts of the system acts as Provider System and the other as Subscriber system and this makes the two parts a bit different and less integrated. The main idea with Multisystem Integration is to enable operation of the Provider system from the Subscriber System and not the other way around. The two parts are engineered locally.

Security Considerations

If a part of the system network is extended via a remote connection the whole connection and both sides of it need to be treated the same way regarding network security, e.g. having the same security level. The protocols used between the nodes on the control network and on the client server network are not designed to be used through a firewall. [Section 5, Network Security](#) describes different alternatives for how to extend the Automation System Network through firewalls.

Multisystem Integration

With the system concept “Multisystem Integration” it is possible to build one automation system consisting of two or more 800xA Systems. This allows for a looser connection between different parts of the system. It is for example possible to have parts of a system operating even if the connection to the rest of the system is not working. The basic idea is to create a separate Aspect Directory for a part of a system that needs to be able to operate on its own. With “Multisystem Integration” the system represented by that Aspect Directory can be operated or supervised from a system represented by a different Aspect Directory.

The supervising system is called the *Subscriber* System and the supervised system is called the *Provider*. Two services implement the communication between the systems; the Remote Access Server running in the provider system and the Remote Access Client running in the subscriber system.

Figure 31 shows two systems that are integrated.

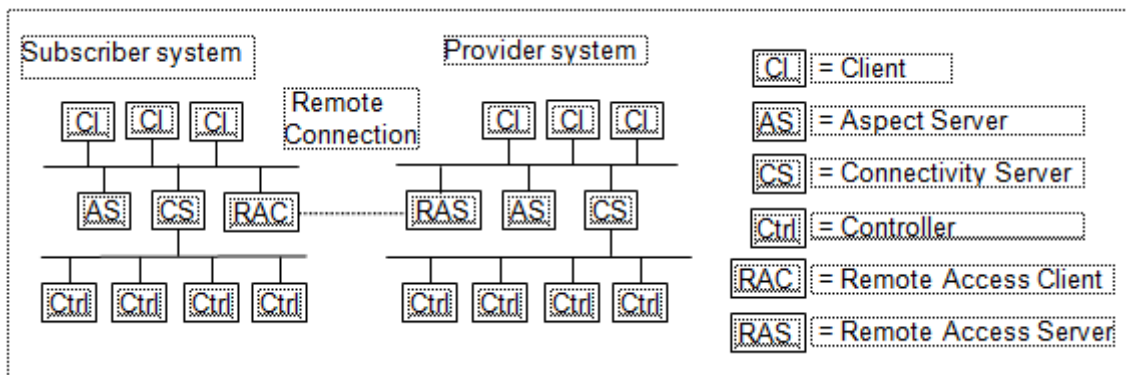


Figure 31. Two integrated Systems: Subscriber and Provider systems

With the Multisystem Integration OPC data from the provider system is accessible in the subscriber system. The opposite is not supported. This means e.g. that clients in the subscriber system can supervise and operate the process in the provider system, but the clients in the provider system can not access the subscriber system.

The network between the subscribers and providers can be everything from a high speed LAN with 100Mbps down to a modem connection with a speed of 128Kbps. The network may be one RNRP network with routing between all nodes in both system but it may also be two separate networks connected via a link where only the Remote Access Client and the Remote Access Server can communicate. Choose the alternative which is most appropriate for the installation.

Password and encryption is used to secure the connection between the provider and the subscriber.

For each connected provider there is a Remote Access Client service group in the subscriber system. A remote Access Server can service more than one subscriber. [Figure 32](#) shows one automation system consisting of one subscriber system and two provider systems.

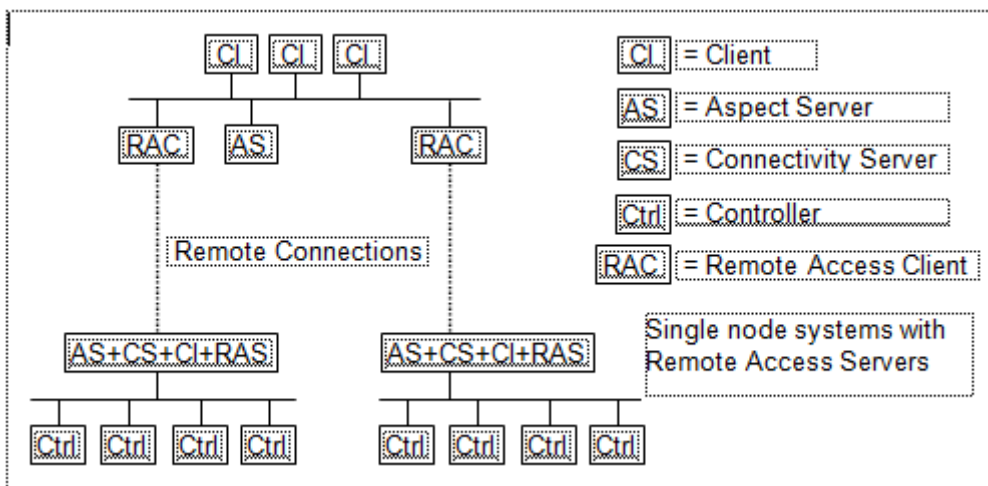


Figure 32. Multisystem Integration: One subscriber system, two provider systems

Which node to run the Remote Access Server and the Remote Access Client in depends on the sizes of the systems. Multisystem Integration is described more in the manual *System 800xA Multisystem Integration (3BSE037076*)*.

Multisystem Integration with redundancy

A redundant integration between two systems can be done using multiple Remote Access Clients and Remote Access Servers. The Service Group for the Remote Access Clients have a list of Remote Access Servers.

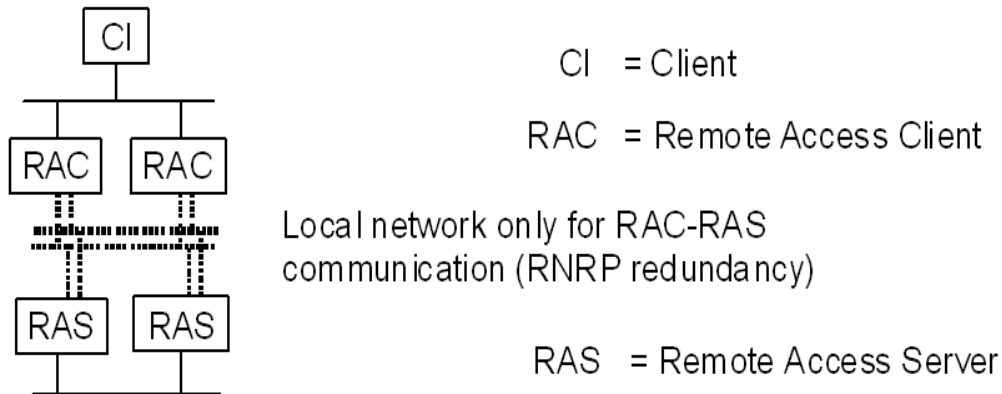


Figure 33. Multisystem Integration with redundancy

The connections between the Remote Access Clients and Remote Access Servers need to allow all Clients to connect to all Servers. These connections may be made redundant using RNRP, but layer 2 redundancy solutions as for example a ring redundancy may also be used.

Using a layer 2 redundancy or using a local RNRP area (see section [Local Network Areas](#) on page 47) does not give routing via the RAC-RAS network. This is normally the recommended solution. This helps segregating the systems, for example RNRP’s network node status events for nodes in one system should be detected inside that system and not show up as events related to unknown objects in the other system.

Using a normal RNRP area between the RAC and the RAS will allow routed communication between the nodes in the two systems for example for remote engineering. If redundancy and routing is desired and the RAC-RAS connection goes via standard routers RNRP Tunnel Areas may be used, see [Interconnecting RNRP Network Areas via Standard IP Routers](#) on page 62.

Asset Optimization

Feature Pack Functionality

Using Asset Optimization with Multisystem Integration, the Condition Reporting and Monitoring, and Work Order Management functions can be performed remotely from the subscriber system.

The following network link between Provider and Subscriber system must be setup to use the Asset Optimization functions in the subscriber system.

1. The Asset Optimization node(s) in the subscriber system must be able to communicate with **AOWebServerNode** in the Provider system. The Asset Optimization Web View aspect uses https/http protocol to communicate with **AOWebServerNode** in the Provider system.
2. If the CMMS Integration is used, then Asset Optimization node(s) in the subscriber system must be able to communicate with the CMMS Web Portal System.

For more information on using Asset Optimization with Multisystem Integration, refer to *System 800xA Multisystem Integration (3BSE037076*)* user manual.

Section 4 Field Networks

System 800xA supports a number of Ethernet based Fieldbuses, a.k.a. Field Networks. The integration of such a network is normally done via a communication module for the AC 800M controller and a connectivity server as indicated below.

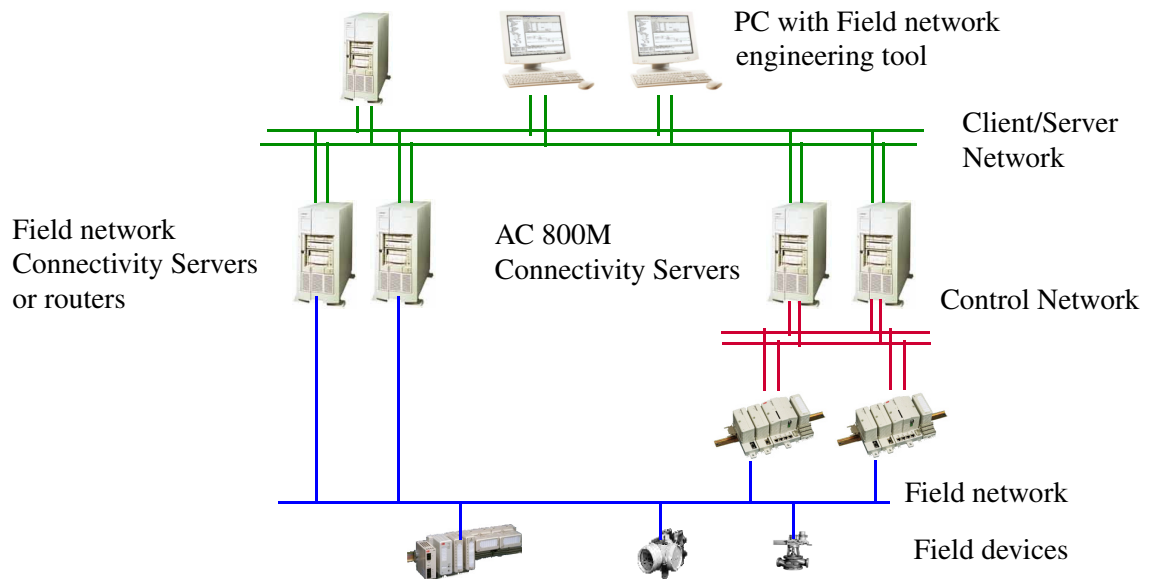


Figure 34. Field network with connectivity servers

This topology provides the following benefits:

- Controllers are directly connected to the Field Network to get real time access to the process data on the field network.
- Data not needed by the controllers is not handled by the controllers. This avoids unnecessary performance degradation of the control application.
 - Operator data goes via the a OPC Servers in the Connectivity Servers.

- Engineering of field devices can be done using the Connectivity Servers as IP routers. Section [Routing from the system network](#) on page 88 describes more about this.
- The Field Network protocol is not used on the Control Network. There are several reasons to keep these separated. See [Coexistence of Network Types](#) on page 218.

Selecting IP Addresses for Field Networks

When planning a system the user must decide what IP addresses to use for all nodes in the system. This also includes the Field Networks. Some things to consider when selecting the addresses for Field Networks:

- Decide which NetIDs to use for the different networks and make a summary of all used NetIDs. One good way of organizing the NetIDs is to use different ranges for different protocols. [Table 7](#) shows one example.
- Normally it is recommended that non-RNRP networks do not use NetIDs that correspond to the RNRP Base Address for the system network. This for example means that if the default base address is 172.16 the NetID 172.16.x and 172.17.x should not be used for a network not using RNRP. [Routing from the system network](#) on page 88 describes an exception to this rule.
- When engineering IEC 61850 with the IET tool the default addresses are “172.net.bsw.unit” where “net” is a network number for a station, “bsw” is a bay number and “unit” is a unit in the bay, e.g. an IED. When using the default network address for the 800xA System Network 172.16.x.y “net” should be set to at least 18 so that the addresses do not overlap.
- Decide which IP addresses to use for the individual devices. One good way of organizing the addresses is to use different ranges for different types of devices/nodes. [Table 8](#) shows one example.

Table 7 gives an example of allocation of IP addresses for different field networks.

Table 7. Example of NetIDs and Subnet Masks for Field Networks

Network Type	NetIDs	Subnet Mask
HSE Subnets (FOUNDATION Fieldbus)	192.168.1.0 - 192.168.40.0	255.255.255.0
Insum	192.168.41.0 - 192.168.60.0	255.255.255.0
Modbus TCP	192.168.61.0 - 192.168.80.0	255.255.255.0
IEC61850	192.168.81.0 - 192.168.100.0	255.255.255.0
PROFINET IO	192.168.101.0 - 192.168.110.0	255.255.255.0
EtherNet/IP	192.168.121.0 - 192.168.130.0	255.255.255.0

Table 8 gives an example of allocation of the Host ID part of the IP addresses for different FF HSE devices.

Table 8. Suggested Node Numbers on an HSE Subnet

Nodes	Node Number/ (Host ID)
Spare	1 - 10
Only to be used temporarily during commissioning (factory defaults of un-commissioned devices will preferably use these node numbers)	11 - 20
Connectivity servers (running OPC Server FF) Let the Connectivity Servers that connect to both the Client/Server Network and the HSE Subnet use the same node number on both Network Areas.	21 - 50
Linking devices	51 - 150
Communication interfaces	151 - 254

Field Network Connectivity Servers

For some of the Field Networks there are connectivity servers. These connectivity servers are for example used for:

- OPC access to data in the field devices
- Network isolation between the Client/Server Network and the Field Network.
- IP routing for one or many nodes on the Client Server Network. See [Routing from the system network](#) on page 88.
- Bridging between RNRPs network redundancy and redundancy on the Field Network.
- Time Synchronization for the Field Network. The connectivity servers are synchronized as all other 800xA nodes. Field devices may use NTP to synchronize from the connectivity servers. For FF HSE this is mandatory.

Details on how to build and use the networks are described in the manuals for the specific field network, see [Protocol specific documentation](#) on page 90.

Routing from the system network

For many of the Field Networks some type of access is desired from nodes on the Client Server Network directly to the Field Network. This is for example for engineering of Field Devices, diagnostics or asset monitoring. To enable this the node on the Client Server network either needs to have an extra network adapter directly connected to the Field Network or to use IP routing from the Client Server Network. For this routing to work there must be at least one node that connects to both networks which is able to act as a router. The node on the Client Server Network that is to use the router needs a routing entry for the Field Network so that it knows that it is the router that it must send the traffic to in order to get to the Field Network. This routing entry can be created manually, e.g. with the command line command “route add”.

If IP routing between the Client Server Network and the Field Network is the only reason for a node between these networks, i.e. no OPC functionality is needed, a standard router or firewall may be used.

If the router is a PC, e.g. a connectivity server, an alternative is to use RNRP. If the Field Network is configured as an RNRP network area RNRP in the router will distribute information about the Field Network and all nodes on the System Network will automatically configure routing entries for the Field Network. If the Field Network is given an address according to the rules for implicit RNRP configuration, i.e. 172.16.x.y this will work automatically. If different addresses are used an RNRP network area can normally be explicitly configured. See [RNRP Address Configuration: Implicit or Explicit](#) on page 50.

If a standard router is used the connection between the engineering tool and the field network may need to be non redundant. If a PC with RNRP is used the redundancy on the Client Server Network can be utilized. If the Field Network provides redundancy the complete routing path may with redundancy.

If RNRP is used for the Field Network it must be made sure that it does not give any problems with the limitations on number of network areas in the system. See [Limit the number of network areas](#) on page 42.

Using RNRP to configure routing for a Field Network has the following +/-:

- + Easier to configure the routing
- + The routed communication can use redundancy
- More RNRP network areas are used
- All nodes on the system network get routing entries for the Field Network. This may be a security drawback.

Independent of how the routing entries are created in the nodes on the Client Server Network the nodes on the Field Network also need routing information about how to reach the Client Server network. Normally this is best handled by setting the parameter Default Gateway in the nodes on the Field Network to refer to the Field Network address of the router.

Network Redundancy

Some Field Networks provide network redundancy. Some networks use a ring protocol (see [Ring Redundancy](#) on page 220). Some use a duplicated network. Study the details on how to handle redundancy in the manuals for the specific field network, see [Protocol specific documentation](#) on page 90.

Physical Field Networks

Some field Networks allow a free selection parameters for the physical network such as of speed and duplex and some do not. For PROFINET IO Auto Negotiation and a speed of 100 Mbps must be supported. In cases where problems are seen that the switch is not working correct, 100Mbps and full duplex shall be configured.

Study the details on the requirements on the physical networks in the manuals for the specific field network, see [Protocol specific documentation](#) on page 90.

Protocol specific documentation

Modbus TCP is described in the manual *System 800xA, AC 800M, Communication Protocols (3BSE035982*)*. For the other Ethernet based protocols there are dedicated manuals:

System 800xA, AC 800M, FOUNDATION Fieldbus HSE (3BDD012903)*

System 800xA, AC 800M, PROFINET IO Configuration (3BDS021515)*

System 800xA, AC 800M, Ethernet IP DeviceNet Configuration (9ARD000014)*

System 800xA, AC 800M, IEC 61850 Configuration (9ARD171385)*

Section 5 Network Security

Network security measures aim at protecting the confidentiality, integrity, and availability of a computer system. This is a complex challenge involving both technical and procedural measures. Providing and managing enterprise-wide network security is a moving and dynamic target, complicated by continuous technical, organizational, political changes, global interconnections, and new business models such as Internet-based e-commerce.

There is no single solution or technology for network security that fits the needs of all organizations and all applications. While basically all computer systems are vulnerable to intrusion attempts, the potential consequences of such attempts are vastly different for different types of applications. The security measures that are applied to a specific installation should be proportional to the assessed risk in terms of probability of an attack and the potential consequences. For a small system with a few users controlling a non-critical process this risk is obviously smaller than for a large system spanning multiple sites with safety critical processes in several countries and continents and thousands or even tens of thousands of users. For manufacturing and control systems in particular, the potential impact of an attack includes, for example, violation of regulatory requirements, loss of public confidence, loss of proprietary or confidential information, loss of production, damage to equipment, and endangerment of public or employee safety.

Establish a Network Security Policy

A key element in implementing and maintaining the security of a computer network is the establishment of an adequate network security policy. This should be based on an analysis and assessment of the needs of the organization, current and planned network structures and information and control flows, risks in terms of probability of different types of attack and potential consequences, and available technical security solutions.

The security policy should be based on the principle of least privilege and compartmentalization, i.e., every application, user, or subsystem should be restricted to the minimum number of rights for the minimum number of resources that is necessary to fulfill its purpose. Network access to functions that are not explicitly required should be disabled. This reduces the possibilities that an attacker can exploit and limits the damage in case an intrusion attempt is successful.

The Onion Approach

A generally recommended approach to network security is the onion approach, also known as “defense in depth”. The inner layers, or zones, of a network, where communication interaction needs to flow freely between nodes, are referred to as trusted. Trusted network zones should be kept small and independent. They need to be physically protected, i.e. physical access to nodes, network equipment, and network cables, must through physical means be limited to authorized persons. When connecting a trusted network zone to outer network zones, additional layers of security measures should be applied, isolating the network zones from each other and providing additional security for the network as a whole.

Firewalls are used to control network traffic between zones of different security levels and to filter out undesirable or dangerous material. Traffic that is allowed to pass between zones should be limited to what is absolutely necessary, because each type of service call or information exchange translates into a possible route that an intruder, virus, or worm may be able to exploit. Different types of services represent different risks - incoming e-mail, as an example, represents a very high risk.

Security mechanisms should not only include defensive and preventive means, but also means for detection and reaction. By continuously monitoring a system for intrusion attempts, users can be alerted to potential threats and take suitable actions, such as isolating an inner network zone from outer zones.

[Figure 35](#) below illustrates how the onion approach could be applied when connecting an 800xA System to an office network, which in turn is connected to Internet.

An overview of different elements of network security, and measures and practices that a user of an Industrial IT 800xA System may want to consider, can be found in the document *IIT Integrated Automation System - Network Security Considerations (3BSE032547)*. The document *Microsoft Security Updates Validation Status* describes which Windows updates that are verified together with the 800xA System. Both these documents are available in the ABB Solutions Bank.

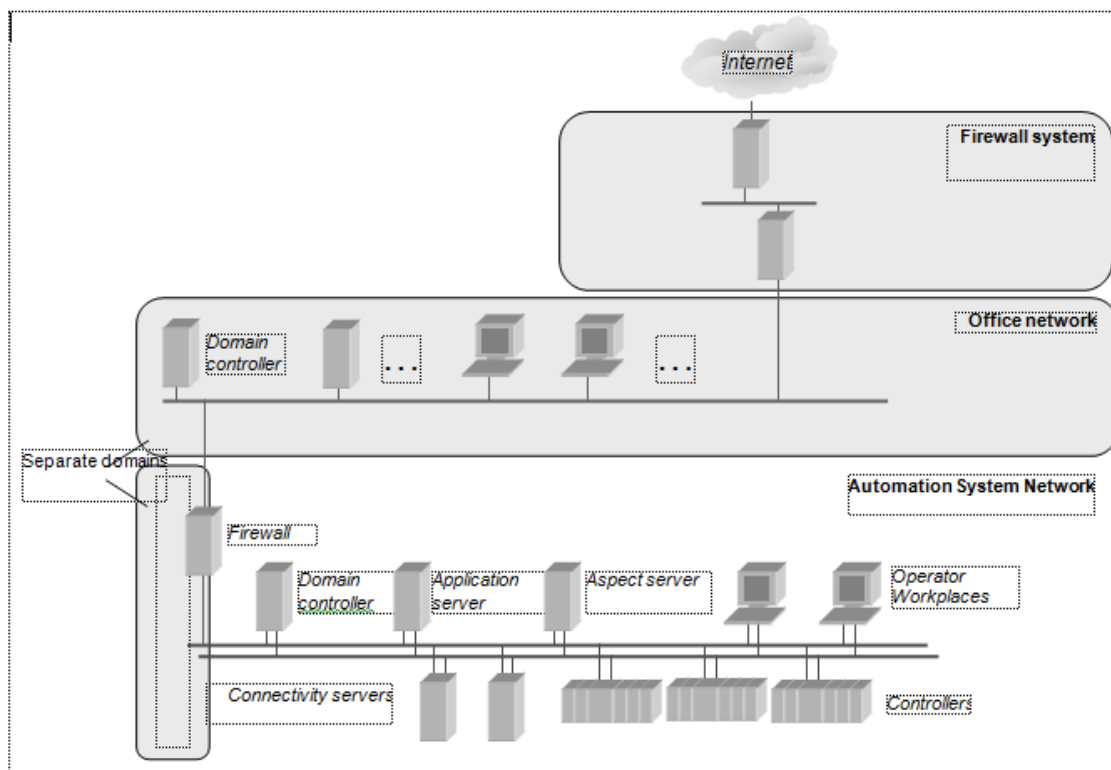


Figure 35. Example of how the Onion Approach could be applied when connecting an 800xA System to an Office Network, which in turn is connected to Internet

All external connections to an Industrial IT 800xA System network should be made through a firewall. Direct connections to nodes in the 800xA System, e.g. through dial-up modems and similar equipment, should not be used.



A connection between the Internet and an Industrial IT 800xA System must always pass through a correctly configured and maintained firewall system.



The security measures described in this document represent possible steps that a user of an 800xA System could consider, based on a risk assessment for a particular application and installation. This risk assessment, as well as the proper implementation, configuration, installation, operation, administration, and maintenance of all relevant security related equipment, software, and procedures, are the responsibility of the user of the 800xA System.

Firewalls

The selection and design of a firewall system should be based on the corporate security policy. It should be revised on a regular basis, as requirements and environment change. Note also that while firewalls block traffic from the outside of a protected area to the inside, they normally allow users on the inside to communicate freely with outside services. For manufacturing and control systems, more restrictive policies are likely to be appropriate.

A firewall system can be a dedicated hardware box, a workstation, one or more servers, or a mix of all of these. There are four general classes of firewall functions:

- Packet filtering firewalls check the address information in each packet before forwarding it to its destination. If this information does not match certain criteria, the packet is dropped. Advantages of packet filtering firewalls include low cost and low impact on network performance. Packet filtering firewalls are also referred to as Static Filtering firewalls.
- Stateful Filtering firewalls are similar to Static Filtering firewalls but they remember outgoing requests („keep state information“) and dynamically reconfigure rules to let responses back in. This often simplifies the firewall configuration, particularly if the connections through the firewall are established only from one side and the traffic from the other side can be considered as responses to accepted requests.

- Stateful Inspection firewalls check packets at the network layer, determine which packets are legitimate, and then evaluate the contents of packets at the application layer. Stateful inspection firewalls offer a high level of security, good performance, and do not require configuration of each node, but are expensive and must be properly configured and maintained, otherwise they can actually be less secure than simpler types of firewalls.

They are sometimes combined with content scanning functions that for example can block viruses, filter out active contents from e-mail, etc. Stateful Inspection firewalls are also referred to as Dynamic Packet Filtering firewalls.

- Application Proxies examine packets at the application layer, and filter traffic based on specific application level rules. They offer a high level of security, but have a significant impact on network performance. They are not transparent to end-users, but require configuration of each client workstation. Application proxies are often combined with a circuit-level gateway, which monitors the TCP handshaking to determine whether a requested session is legitimate. Application proxies are well suited to use in association with a demilitarized zone, see [Single Firewall or a Demilitarized Zone](#) on page 99. There are a number of examples of Application Proxy solutions that are suitable for an 800xA System. A particular firewall may contain a combination of these functions:
 - Web Proxy
A web proxy is an application that forwards http traffic. Clients on the 800xA System network only access the web proxy. From the outside it looks like all traffic comes from the web proxy. This can be used for all http traffic. General web access to the Internet might not be desired from the 800xA System but some integrations with 3rd party systems use http, see [Integration with 3rd Party Systems](#) on page 113.
 - Remote Client access in two steps
This is perhaps not a real proxy application but it serves the same purpose. See [Remote Clients Connecting through a Demilitarized Zone](#) on page 112.
 - Remote access via Separate Subscriber System
Multisystem Integration can be used to create an intermediate node that is accessed from the outside. See [Subscriber system as Application proxy](#) on page 115.

Besides filtering network traffic, firewalls normally also log communication events and intrusion attempts. It is recommended that the security policy contains a plan for if and how to use this information.

Firewall systems are available for example from:

- Checkpoint (www.checkpoint.com)
- Cisco (www.cisco.com)
- Netscreen (www.netscreen.com)
- Nokia (www.nokia.com/securitysolutions).

Connections to 800xA Systems through Firewalls

This section describes some general background information which is true for many different applications that require access through a firewall.

Connect Inside-out Instead of Outside-in

Connections between the 800xA System and other systems through a firewall may be done in different ways depending on the direction. It is easier to maintain a high level of security if connections are only allowed from the automation system network out to the external network and not vice versa.

If you need to get data from the 800xA System to an external system it is better if you can push the data from the inside of the system instead of allowing for an external system to fetch the data from the outside. An example is described in [Using a 3rd Party Access Agent](#) on page 114.

Network Address Translation in Firewalls

In addition to configuring access restrictions by port numbers, it is recommended to configure the firewall to perform Network Address Translation (NAT).

This prevents externally exposing the IP addresses used in the 800xA System.

If the only connections that are needed through the firewall are initiated from the automation system network the firewall only needs to expose its own external address to the external network. All connections will look like they were initiated from within the firewall.

If there is a need for applications on the external network to connect to servers on the automation system network the firewall needs to expose more addresses to the external network. This can be done using “static NAT”. Static NAT means that the firewall translates between static pairs of external and internal addresses. For each individual server that is to be accessed from the external network the firewall needs to expose an address in addition to the firewalls own address on the external network. See [Figure 36](#).

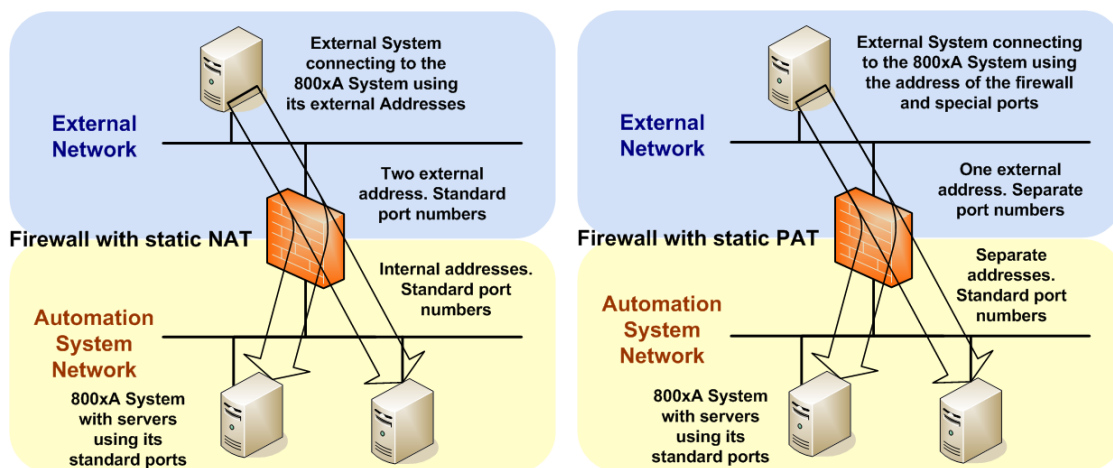


Figure 36. Static Network Address Translation or Port Address Translation

An alternative to NAT is PAT (Port Address Translation): The Firewall only exposes one IP address but is configured to forward traffic directed to specific ports on its external network interface to another port on a node on the automation system network. A separate external port number is reserved for each local server. To be able to use PAT it must be possible to configure which port the external clients should connect to.



By usage of Network Address Translation the addresses used by the 800xA System do not need to be known anywhere except internally on the automation system network. This makes it possible to use the same address range (see [Recommended IP Address Plan](#) on page 30 and [Choosing Address Space](#) on page 249) for each 800xA System even if there are more than one 800xA System connected to the same external network and even if they need to be accessed from outside or even need to access each other.

Example:

Two Terminal servers on the Client Server Network to be used by remote clients on the plant network.

Static PAT: If the port numbers, used by the Terminal Clients when they connect to the Terminal Servers, can be changed it is not necessary to expose any other addresses for the Plant Network than the address of the Firewall (10.1.1.101). The Terminal Clients select which Terminal Server to use by selecting different port numbers (33389 or 33390). The Firewall translates access towards 10.1.1.101:33389 to 172.16.4.41:3389 and 10.1.1.101:33390 to 172.16.4.42:3389.

Table 9. Address translation rules, Static PAT

Node	Internal		External	
	IP Address	Port #	IP Address	Port #
Firewall	172.16.5.245		10.1.1.101	
Terminal Server 1	172.16.4.41	3389	10.1.1.101	33389
Terminal Server 2	172.16.4.42	3389	10.1.1.101	33390

Static NAT: If it is desired not to set any special port numbers for the Terminal Clients it is necessary to expose specific IP addresses for the Terminal Servers on the Plant Network.

The Terminal Clients select which Terminal Server to use by selecting different IP addresses (10.1.1.141 or 10.1.1.142). The Firewall translates access towards 10.1.1.141:3389 to 172.16.4.41:3389 and 10.1.1.142:3389 to 172.16.4.42:3389.

Table 10. Address translation rules, Static NAT

Node	Internal		External	
	IP Address	Port #	IP Address	Port #
Firewall	172.16.5.245		10.1.1.101	
Terminal Server 1	172.16.4.41	3389	10.1.1.141	3389
Terminal Server 2	172.16.4.42	3389	10.1.1.142	3389

Single Firewall or a Demilitarized Zone

A connection between an Automation System Network and an external network should be done through at least one firewall. The solution may be done more or less complex depending on the requirements on the security.

A simple straight forward solution is to use one firewall with two network interfaces, one connected to the 800xA System Network, one interface is connected to the external network, see [Figure 37](#). Configure the firewall to only allow the necessary services to pass. The instruction *System 800xA Engineering Planning (3BSE041389*)* contains a number of points to consider when planning how to configure the firewall.

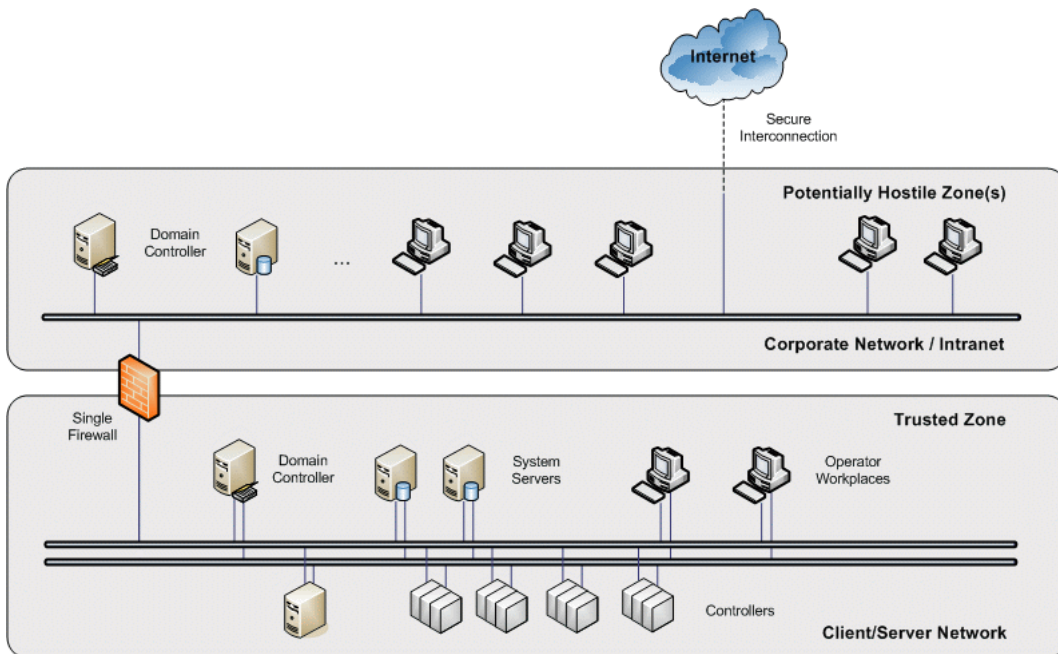


Figure 37. Single firewall between 800xA and external network

By using a firewall with more than 2 network interfaces it is possible to build a solution where one interface is connected to the 800xA System Network, one interface is connected to the external network and at least one port is connected to a separate network that may be called “Demilitarized Zone” (DMZ), [Figure 38](#).

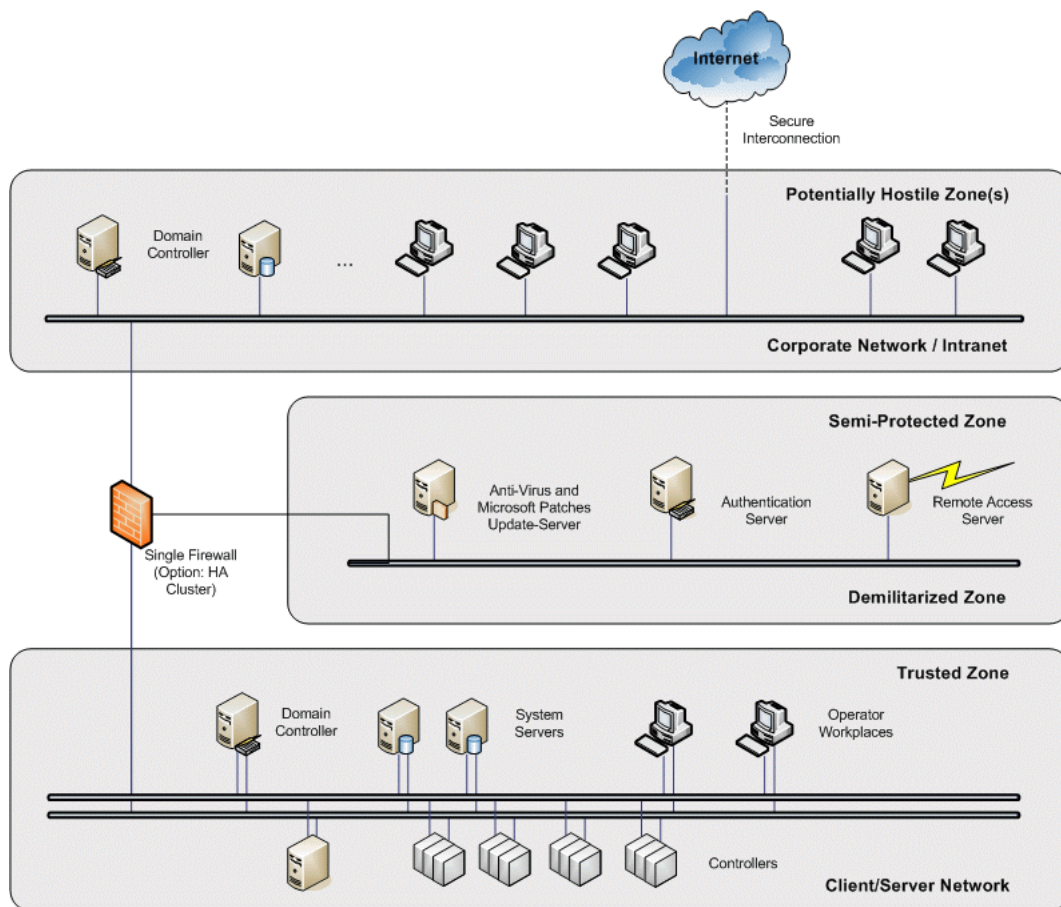


Figure 38. Firewall with demilitarized zone between 800xA and external network

The idea with a Demilitarized zone is that the traffic between the external network and the 800xA System needs to go via nodes on the demilitarized zone. Connections should not be made directly between an external node and a node on the 800xA System network. Exactly how this can be done depends on the actual service which is to be accessed.

One example is that anti virus updates and security patches can be loaded to a server in the demilitarized zone and fetched from that node from the system network. For some services there are Application proxies (see [Firewalls](#) on page 94) that can be connected in the demilitarized zone.

Another common usage of a demilitarized zone is as the location of VPN gateways for VPN connections terminated outside the Automation System Network, see [Figure 43](#) on page 107.

By using two firewalls of different types the security of the demilitarized zone can be built even stronger, see [Figure 39](#). If there is a problem with the firewall on the outside of the demilitarized zone there is still a chance that this can be detected allowing actions to be taken before there is a problem also with the firewall on the inside. The nodes and services to connect to the demilitarized zone can be the same in this solution as in the previous one. A further extension could be to use different demilitarized zones for different services.

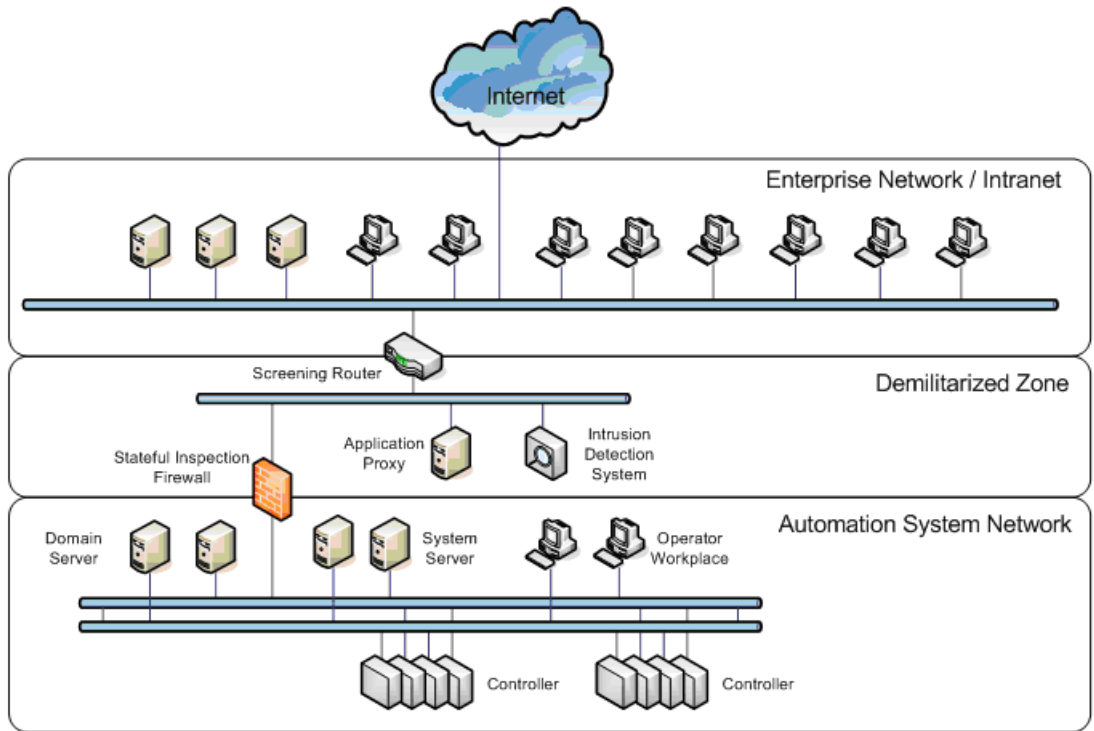


Figure 39. Dual firewalls with demilitarized zone between 800xA and external network

Connecting a single Firewall to a Redundant Network

Two basic approaches can be used to connect a firewall to a redundant network using RNRP. The two methods plus a variant of the second are shown in Figure 40.

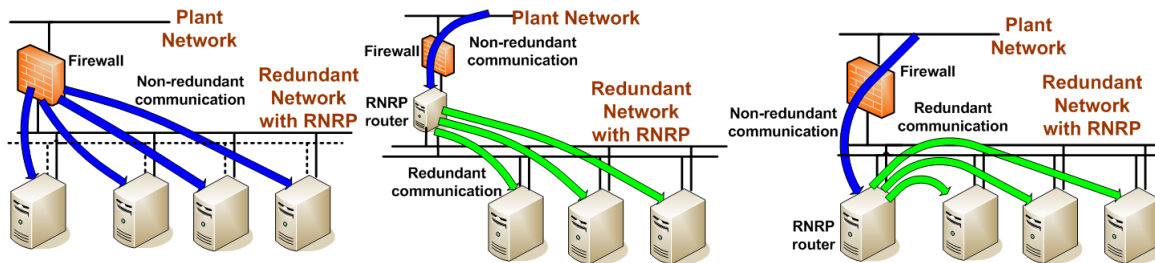


Figure 40. Connecting directly on the primary network or via an RNRP router

- Left: Connect the firewall to the primary path of the redundant network and let it communicate directly to all nodes it needs to reach. In this case the firewall can only communicate with nodes for which the primary network path is working OK. If a node loses the primary path the firewall can not reach it.
- Middle: Use a server running RNRP as router between the redundant network and the firewall. In this case the firewall can communicate with nodes even if they lose the primary network path. It is however dependant on the RNRP router node to work OK.
- Right: The middle solution can be slightly modified to save some hardware: The router node does not need to use 3 network interfaces. It is possible to do the connection between the router node and the firewall using the primary network. This (or the middle) method is recommended at least when a tunnel area is used (see [Interconnecting RNRP Network Areas via Standard IP Routers](#) on page 62) since this anyway requires an extra router node: the tunnel area border node.

Using an Extra Network for Remote Access

To separate the network traffic for remote access from the normal traffic on the Client Server network a extra network can be built for this traffic between the firewall and some of the 800xA nodes. An example is shown in [Figure 41](#).

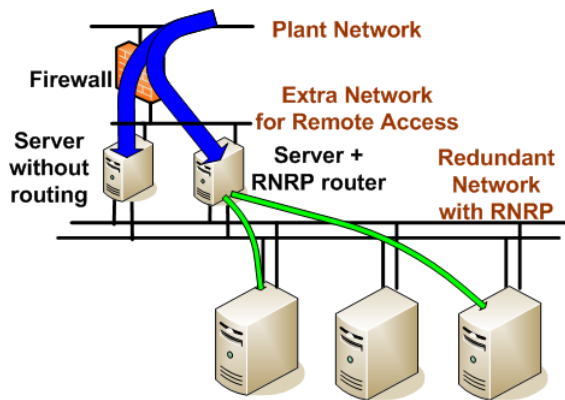


Figure 41. Extra network for remote access limiting the Client Server network traffic

This is particularly useful if there is much traffic for remote access and if only a few internal nodes are to be accessed from the outside, for example some terminal servers for Remote Clients. Connect only the nodes that will have much remote access traffic to the extra network. If needed the other nodes can be reached via one of these nodes that will act as a router as in the middle alternative in [Figure 40](#) on [page 104](#). Disable IP forwarding in the other nodes.

This method provides some degree of improved security since it limits the amount of remote access traffic on the Clients Server network.

Redundant connection to external network

RNRP redundancy can be combined with other routing redundancy protocols. Using firewalls with VRRP and OSPF together with RNRP routers running OSPF it is possible to create a fully redundant connection to an RNRP network.

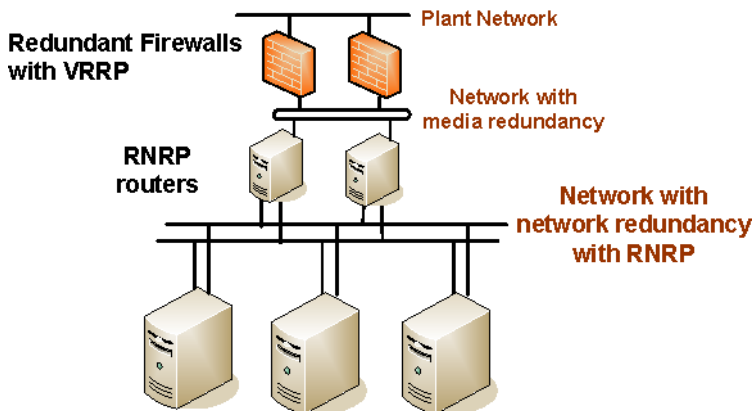


Figure 42. Redundant firewalls connected to Redundant Client Server Network

Virtual Private Networks (VPN) for Secure Connections

Virtual private network (VPN) is a general notion for a connection that is created over an existing public or shared network using encryption and/or authentication technologies to protect the user data. The two main applications for VPNs are:

- VPN for LAN to LAN connections. Two secure networks are connected via an encrypted connection over an unsecure network. The most common protocol to use is IPsec. This type of VPN can be used for all kind of IP based communication. An application is described in [Site to Site Connections via a Firewall](#) on page 112.
- VPN for remote access. A remote client node is connected to a server on a local network. IPsec and SSL are commonly used protocols for remote access. IPsec operates on the network layer and is thus able to protect all UDP- or TCP-based communication, but requires appropriate configuration of the firewalls by the network administrators. SSL operates on a higher protocol layer and only

protects TCP-based connections. It requires that users or application software handle digital certificates, but has typically less interaction with networking and firewalls than IPsec.

[Secure Connections for Remote Clients](#) on page 111 describes considerations on VPN usage for remote access.

A VPN connection to a network is terminated in a VPN gateway. Many firewalls can act as VPN gateways.

A VPN connection typically does not filter traffic. This means that both sides of the connection need to be treated the same way regarding network security, e.g. having the same security level. A VPN connection to an 800xA System should only be terminated in a VPN gateway connected directly to the system network if the other side of the connection has the same security level. An alternative is to terminate the VPN connection in a VPN gateway connected to a network outside a firewall and to let the communication between the VPN connection and the system network go unencrypted through the firewall to the system network. This way the traffic from the VPN connection can be filtered before entering the system network. If a demilitarized zone (DMZ) is used outside the Automation System Network the VPN gateway can be placed in there (see [Single Firewall or a Demilitarized Zone](#) on page 99).

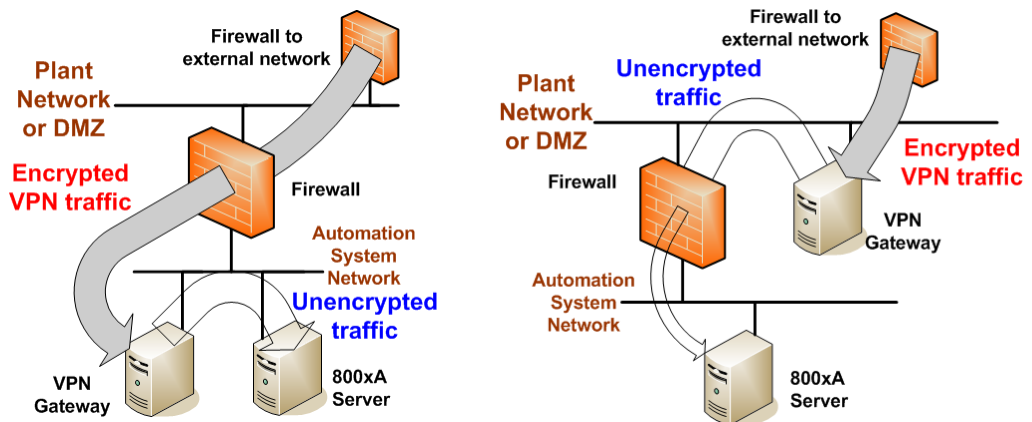


Figure 43. Terminating the VPN inside or outside the 800xA System Network

Use cases for Connections through Firewalls

From network security point of view the easiest configuration to maintain is an isolated Automation System Network which is not connected to any other network. There are however a number of cases where it is necessary to connect the Automation System Network with some other network.

Some of the more common use cases are described below:

- **Remote/external client**
The 800xA System needs to be accessed from a user on a computer which is not connected to the automation system network. This means that the Automation System Network needs to be connected to an external network and the client functionality needs to be made available through some kind of firewall system.
This is described in [Remote/External Client](#) on page 109
- **Site to site connection**
The automation system is located on two or more geographical sites and the remote connection needs to go via an external network.
This is described in [Site to Site Connections via a Firewall](#) on page 112.
- **Integration with external 3rd party system**
Data in the 800xA System needs to be accessed from a 3rd party system on an intranet. This can be done in some different ways where the intranet and the Automation System Network are connected in some way.
This is described in [Integration with 3rd Party Systems](#) on page 113.
- **Management of system updates**
Updates for Windows and updates for the 800xA System need to be introduced in the system a safe way.
This is described in [Management of System Updates](#) on page 117.
- **Other services to route through the firewall**
In some cases it may be desired to route some other specific services through a firewall. Some examples are:
 - DNS for name resolution
 - E-mail alerts from an Alarm Server
 - Time synchronization via SNTP or NTPThis is described in [Other Services to be Used Through a Firewall](#) on page 119.

Remote/External Client

It is possible to use client functionality on nodes outside the 800xA System network. The way this should be done depends on what type of client functionality to access:

- External node working with the same functions as the client inside the system, e.g. with the Operator Workplace. This is a case where the external node is used for interactive operation with data which stays inside the system. It is not a matter of extracting data from the system to use in any external system or to import data to the system. The recommended method is to use some kind of remote windows workplace functionality, e.g. Windows Terminal Server and Remote Desktop.
- A user on an external node remotely controls a node on the system network.
- External user accessing OPC data from the 800xA System using Excel and the Information Manager Desktop Tools.

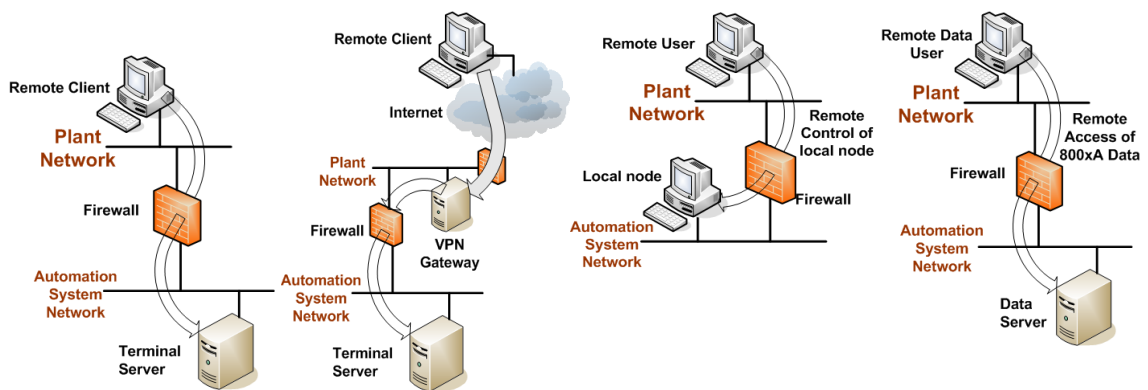


Figure 44. Examples of Remote Client access

The following sections will describe these use cases in more detail. For each use case it will be described which network ports that are needed to be opened in the Firewall.

Remote Windows Workplace

There are two main alternatives for system configurations with a terminal server on the 800xA network to be used by a number of remote clients:

- Microsoft Remote Desktop
The Remote Desktop functionality is included in the standard Windows 7 and Windows Server 2008. The traffic is encrypted.
The default port is 3389 but it can be changed.



Do not select Local Resources as Printers, Drives and Remote computer sound when establishing a remote desktop session towards an 800xA node as there is a possibility of performance degradation on the target node.

- Citrix
Citrix remote clients can be configured to use a number of different protocols:
 - Citrix Client, no encryption. Uses port 1494 for a proprietary protocol.
 - Citrix Client, secure connection. Uses port 443 for HTTPS.
 - Web Browser. Uses port 80 for HTTP and 1494 for a proprietary protocol.
 - Web Browser, secure connection. Uses port 80 for HTTP and 443 for HTTPS.

Remote Usage of a Node on the System Network

There are a number of products that allow a remote user to use a node on the 800xA System Network. With these products the server node is taken over by the client. This can for example be used for remote administration of a system or for assistance to local engineers.

- VNC
VNC is an open source protocol. There are several implementations, e.g. RealVNC, TightVNC and UltraVNC.
All implementations do not support encryption.
The default port number is 5900 but it can be changed.
- Symantec PC Anywhere
The default port number is 5631 and 5632 but it can be changed.

To enable remote usage of all nodes in a system it might be good to do these connections in more than one step. Establish one connection from the remote node to one particular node on the system network and connect from that node to the

other node. This makes it easier to configure the firewall if it only needs to allow connections to one local node.

Information Manager Desktop Tools

The Display Services Client, Desktop Trends and the Excel addins are functions that make it possible to work with data from the 800xA System. They are normally installed on a PC which is not part of the 800xA System. To use these tools on a node on a plant intranet outside a firewall the ports 19014-19017 need to be opened for access from the external node to the Information Manager server. The port numbers can be changed.

Secure Connections for Remote Clients

To run Client functionality on an external node a connection from the external node needs to be established to a node on the 800xA System network. This connection may be done more or less complex giving different level of security.

Many of the products providing Remote Client functionality support encryption between the client and the server. In some cases this might be considered sufficient, e.g. if the clients are located on a protected plant intranet. If a higher level of security is desired the connection may be done using some kind of additional VPN connection see [Virtual Private Networks \(VPN\) for Secure Connections](#) on page 106.

If a remote node is connected as a client to an 800xA System via a VPN connection it is very important to notice that the same care must be taken regarding the security handling of the remote node as for the 800xA nodes since the VPN connection may make the remote node a member of the 800xA System and if the remote node is unsecure the whole system may be unsecure. For example the remote node should preferably not have any normal connection to Internet when it is connected to the 800xA System.

A way to limit the risk from a remote client is to make sure that the remote client only has access to a limited set of services. This can be done by using a remote client application that only has a limited set of services instead of using a VPN connection that gives the remote client the same rights and possibilities as a local node in the system.

Remote Clients Connecting through a Demilitarized Zone

A remote client connection through a demilitarized zone can be done as a two step connection: One remote client connection from the external network to a terminal server on the Demilitarized zone and another remote client connection from that node to a terminal server on the 800xA System network. If the two connections are done using different products the risk for intrusion due to problems with one product is reduced, but some combinations of some products may however not work perfectly. There may for example be problems with keyboard handling.

Site to Site Connections via a Firewall

Two parts of an automation system that need to communicate via a network with lower security level than the automation system network can use a VPN for LAN to LAN connection (see [Figure 45](#) and [Virtual Private Networks \(VPN\) for Secure Connections](#) on page 106).

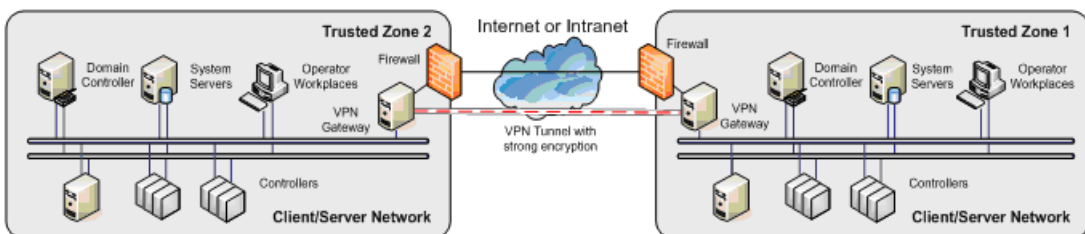


Figure 45. Site to Site VPN

The VPN connection tunnels all communication so that it can not be intercepted by any node between the two sides. Filtering of the traffic between the two sides does not need to be done since both sides are regarded as being on the same trusted

network. If filtering is desired the VPN connections may be terminated outside of a firewall on either of the sides as described in [Figure 43](#) on [page 107](#).

The two sides communicating via the VPN connection may be one 800xA System with an extended automation system network with some distributed nodes as some of the examples in [Section 3, Distributed System Topologies](#).

If the connection between the sites needs to be redundant this can be achieved with two RNRP tunnel areas, see [Figure 46](#). See also [Figure 14](#) in [Interconnecting RNRP Network Areas via Standard IP Routers](#) on [page 62](#)

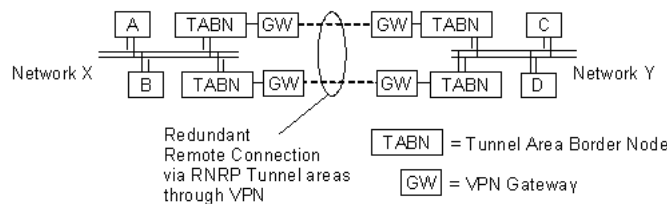


Figure 46. Redundant RNRP Tunnel Areas

The function Multisystem Integration (see [Section 3, Distributed System Topologies](#)) provides an encrypted connection between the systems, so if this is used it might not be necessary to set up a VPN connection between the systems. The Remote Access Client in the Subscriber System needs to be able to communicate with the Remote Access Server in the Provider system via a port which by default is TCP port 3340, but it can be changed.

Integration with 3rd Party Systems

This section describes some of the more common use cases where the 800xA System needs to exchange data with a 3rd party system. Data that needs to be exchanged may be:

- OPC Output data, e.g. from an Information Manager Server, from the 800xA System for further processing.
- OPC Input data controlling the operation of the 800xA System.

- Asset Optimization information to and from an external maintenance management system.

Accessing OPC Data from External Network

Accessing OPC data in the 800xA System is done via the OPC Server interface which is available in all 800xA nodes. The access is done via an OPC Client. It is recommended that the OPC Client is run in the same node as the OPC server or at least in another node on the Client Server Network. If the OPC Client and the OPC Server are run in different nodes they will communicate with DCOM and DCOM is not recommended to be run through a firewall.

ODBC/OLE/DB Access of Data in the 800xA System

The Oracle database in the Information Manager server can be accessed from a node outside the Automation System Network. To do this the external node needs to be able to connect to the Information Manager Server via TCP port 1521.

The Information Manager Server also provides the Open Data Access interface which can be used for accessing historical and process data. An external node using this interface needs to be able to connect to the Information Manager Server via TCP port 1706.

Using a 3rd Party Access Agent

For some 3rd party systems there are access agents that can be installed in a node on the Client Server Network accessing data from the 800xA System and transporting it to its main server via a protocol better designed for communication through a firewall than what DCOM is, see [Figure 47](#). This is in line with the recommendation to establish connections from the inside instead of from the outside, see [Connect Inside-out Instead of Outside-in](#) on page 96. An example is that Aspentech has an access agent for their IP21 server.

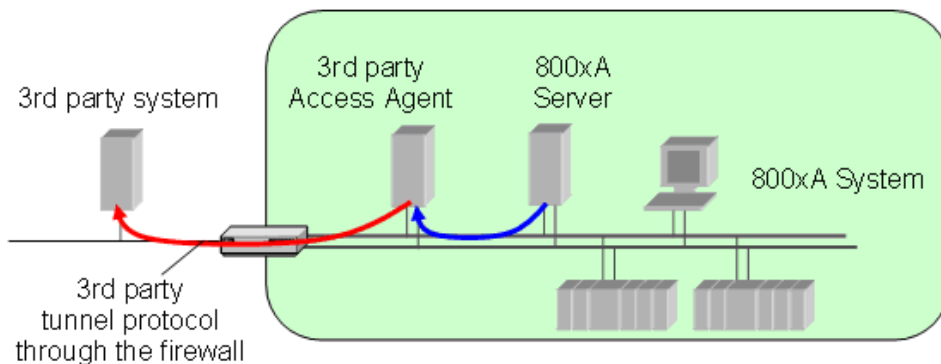


Figure 47. Using an Access Agent through a Firewall

Subscriber system as Application proxy

Another alternative for allowing external access to OPC data is to create an external 800xA System which is connected with Multisystem Integration, see [Section 3, Distributed System Topologies](#).

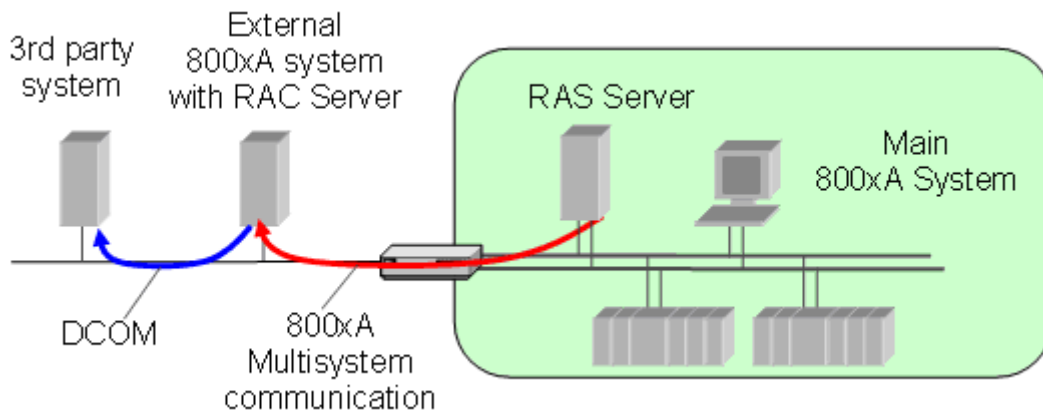


Figure 48. External Subscriber System accessing through a Firewall

The 3rd party system only accesses the subscriber system.

The external subscriber system can be considered as an application proxy for the 800xA System. This approach can for example be suitable in a configuration with a demilitarized zone.

Asset Optimization Integrations

There are a number of 3rd party systems for which there are integration functionality available in the Asset Optimization package. These are:

- **MAXIMO**
A MAXIMO server can be connected to an external network.
It must be possible for the AO Server to reach the MAXIMO server via TCP port 1099. Other 800xA nodes where the user will work with MAXIMO data only communicate with the AO Server.
- **DMS**
A DMS server can be connected to an external network.
It must be possible to reach the external DMS Server via TCP port 80 from any 800xA node where the user will work with DMS Device Management Data and it must be possible for the external DMS server to reach the AO Server via TCP port 80.
- **SAP/PM**
An SAP server can be connected to an external network.
It must be possible for the AO Server to reach the SAP server via TCP port 3300. Other 800xA nodes where the user will work with SAP data only communicate with the AO Server.

All Asset Optimization web services use TCP/IP port 80 by default.

Maximo and SAP Portal Views

Maximo and SAP portal views are function-related web pages viewed in a browser and as such are subject to the security settings configured on the 800xA network. The ability to access and view the web of the Maximo or SAP server is dependent on the 800xA network configuration and the access privilege of the client machines on each server in the network.

A client browser must be able to “ping” a server in order to have the first level of access to the server's web and data. In some networks, a router must be used to allow clients in an 800xA System (nodes) to access servers that are outside the network segment. In particular, servers that are located behind a firewall, may require special access on TCP/IP port 80, or whatever port the HTTP web service is configured to run on.

Batch Integrations

With the function Batch Scheduling Interface it is possible for an external node to access data from the Batch system. The Batch Scheduling Interface is installed on one of the Batch client nodes in the 800xA System. The external node needs to be able to communicate with that node via port 80.

Management of System Updates

Updates of software for the 800xA System, including operating systems, 800xA software, libraries, and applications, are normally done via CD or DVD. Care should be taken to verify that the CD/DVDs are of proper origin and do not contain viruses.

Alternatively, updates could be downloaded from trusted servers on the Internet. The following is an example of a process that could be used. The system administrator for the 800xA System downloads updates from a trusted server on the Internet to a node on the office network.

After verifying the authenticity of all downloads, e.g. by means of digital signatures, and scanning them for viruses, the administrator makes them available on a distribution server on the office network or in a demilitarized zone if such a configuration is used.

From there they are accessed from e.g. an engineering workplace on the 800xA client/server network. In this case the firewall must be set up to also allow this traffic. Configure with a restricted host list, allowing access to the distribution server only.

There are a number of different methods for file transfer from a server. FTP in active mode can not be used through a firewall using NAT. FTP in passive mode may be used, but it requires opening access from the 800xA node to the external server via TCP port 21 and additionally all high TCP ports (above 1023). This is normally not any major problem. It still follows the rule to access from the inside, but FTP uses unencrypted passwords so it is better to use other protocols, e.g. HTTP, HTTPS or SSH for file transfer.

Using WSUS for Windows Updates

The handling of Microsoft Windows security updates can be simplified using Microsoft Windows Server Update Services, WSUS. It must however be used with caution. These are some recommendations of how to use it:

A local WSUS server shall be placed on the Client Server Network. This server may be configured to fetch updates from an external WSUS server. This can preferably be done in several steps with an intermediate WSUS server in a demilitarized zone. The communication between WSUS servers is done via http or https, i.e. port 80 or port 443 need to be opened in the firewalls. Open only for the known WSUS servers, not for all nodes.

The WSUS shall download all updates automatically but it must be configured so that no updates are approved by default.

It is recommended to organize the rules for approvals as groups related to the different System versions since the list of approved updates are organized this way, e.g. by naming the groups as the system versions.

Approvals to the groups shall be made based upon the latest revision of the document Microsoft Security Updates Validation Status for IIT System 800xA, 3BSE041902.

All PPA nodes shall be configured to download updates but not to install them automatically. Use the option “Download and notify for installation”. This can preferably be done with a Group Policy.

Installation of updates shall be performed carefully to ensure that restarts are minimized and are done at well selected times. It is recommended to do it on clients first, non-critical servers next and critical servers last.

Using ePO for McAfee updates

Virus definition updates for McAfee can be centralized using ePolicy Orchestrator (ePO). As for WSUS (see previous section) the recommendation is to have a local ePO server on the Client Server Network with a secure connection to one or a chain of external ePO servers.

ePO uses http for the communication between servers and client components. The port numbers can be changed from 80 and this is recommended to do to use dedicated ports for ePO.

When using ePO the same rules shall be implemented as when handling updates for McAfee manually. These are described in the document *Using McAfee VirusScan® Enterprise with System 800xA, 3BSE048631*.

Other Services to be Used Through a Firewall

In addition to the services mentioned there are a number of other services that may be needed to use through a firewall:

- **DNS**
If nodes on the 800xA System need to address external nodes by host name DNS might be used, but this requires a configuration of the local DNS server on the 800xA System network which is not the standard. It is normally recommended to address any external node by its IP address.
If the external nodes need to be addresses by host name the local Domain Controller needs to be able to communicate with an external DNS Server via UDP port 53.
- **E-mail for alarm alerting**
If the Alarm server will be set up to send e-mails it needs to be able to communicate with the external mail server via TCP port 25.
- **Clock Synchronization via NTP or SNTP**
If real time clocks in the 800xA System will be synchronized from an external NTP or SNTP server the client node on the 800xA System network needs to be able to communicate with the NTP server via UDP port 123.
- **File transfers.** See [Management of System Updates](#) on page 117.

- MMS
The client needs to be able to reach the server via TCP port 102.
- SattBus on TCP/IP uses UDP port 2999.

Summary of Ports to Open in Firewalls

Table 11 is a summary of ports that may need to be opened in a firewall between the 800xA System network and an external network.:



Open only the firewall ports for the functions that are really used!

Table 11. Summary of Port Numbers that may need to be opened

Function	Server Ports	Direction of Connection establishment
Multisystem Integration	3340/tcp	Remote Access Client-> Remote Access Server
Microsoft Remote Desktop	3389/tcp (RDP)	External Client -> 800xA Terminal Server
Citrix remote client	1494/tcp	External Client -> 800xA Terminal Server
Citrix remote client (secure connection)	443/tcp (SSL)	External Client -> 800xA Terminal Server
Citrix web browser	80/tcp (HTTP) 1494/tcp	External Client -> 800xA Terminal Server
Citrix Web Browser (secure connection)	80/tcp (HTTP) 443/tcp	External Client -> 800xA Terminal Server
VNC	5800/tcp (VNC)/ 5900/tcp (VNC)	External Client -> 800xA node to control
PC Anywhere	5631/tcp and 5632/tcp	External Client -> 800xA node to control
SMS & e-mail Messaging	25/tcp (SMTP)	Aspect Server -> External Mail Server
IM, Multi-screen Display Interface and Desktop Trends	19014- 19017/tcp	External Client -> IM Server

Table 11. (Continued) Summary of Port Numbers that may need to be opened

Batch Schedule Interface	80/tcp (HTTP)	External node -> Batch Client
AO, MAXIMO integration	1099/tcp	AO Server -> MAXIMO Server
AO, DMS Calibration integration	80/tcp (HTTP)	Device Management Client -> DMS Server
	80/tcp (HTTP)	DMS Server -> AO Server
AO, SAP/PM integration	3300/tcp	AO Server -> SAP Server
Clock Synchronization	123/udp (SNTP)	Local Time Server -> External Time Server
Download of software updates via passive FTP	21/udp (FTP) >1023/udp	Local File Server -> External File Server
MMS	102/tcp	Client -> Server
SattBus on TCP/IP	2999/udp	Sender -> Receiver

AC 800M Network Storm Protection

A network storm can have different reasons. Network packets can loop because of a temporary or permanent problem in the network infrastructure or the system may be target for Denial of Service attack.

From version 5.1.0/1 AC 800M has a Storm Protection function that replaces RNRP's Loop Protection. The Storm Protection is capable of protection the controller from all types of excessive network traffic that potentially could harm the execution of the control application, not only network storms caused by loops.

The storm limits, i.e. the packet rates at which the storm protection reacts, are different on different Processor Module types.

For PM86x the storm protection reacts if more than 800 packets per second are received. For PM891 the storm protection reacts if more than 1600 packets per second are received.

When the Storm Protection detects excessive network traffic the corresponding network port is disabled for a few minutes. If a redundant network is used the legitimate traffic can continue on the other network. After the port is opened again

and if there still is excessive network traffic the port is closed again. This repeats as long as there is a network storm on one port.

A network loop may cause so high CPU load that the storm protection function itself is not able execute. This means that it can't be guaranteed that the Storm Protection will manage to protect a controller from shutting down.

The Storm Protection improves the possibilities for a node to handle a network loops or Denial of Service attacks, but it does not guarantee that a controller can survive all types of storms.

Section 6 Domain Setup and Name handling

This section describes the domain setup and name handling in the 800xA 5.1 System.

Node name handling and DNS

In 800xA 5.1 System, 800xA uses a combination hosts files and DNS for address and name resolution:

- The resolution of names and IP addresses in the 800xA System is primarily handled via the hosts file in each node.
The host files are updated by RNRP. This is described in [Configuring Name Resolution and DNS](#) on page 125.
- DNS will normally not be used for host name resolution, but in a domain based system it will be used for other Domain Controller related functions such as locating servers for Domain Controller services.
- Only the IP addresses for networks used for Client Server communication shall be resolved to node names.

Choosing Names for Domains and PCs

Before you set up the Domain you should decide the conventions for node names in the system. The first thing to decide is the domain name. The domain will be given two types of names:

- The fully qualified domain name (FQDN)
This is the name that is used by DNS. It can consist of several labels separated by dots, e.g. MyProcess.MyPlant.com.
- The NetBIOS name
This name is used by most Windows components, e.g. the Windows Login

Screen. It is typically equal to the left most part of the fully qualified domain name, e.g. MYPROCESS.

A NetBIOS name cannot be longer than 15 characters. This means that the left most part of the fully qualified domain name must also not be more than 15 characters.

Once an 800xA System has been installed in a domain, the domain name must not be changed. One reason is that user names in the system contain the domain name. Avoid using names that become irrelevant. Remember that for example company names might change.

The name of a domain for a private network that is not going to be connected to Internet should end with “.local”, e.g. MyPlant.local. The part before “.local” can be chosen arbitrarily.

The nodes within a domain must be given computer names that are unique within the domain. The full computer name of a PC is “computer name”.domain name”, e.g. ServerA.mydomain.local (see also [Figure 49](#)). The corresponding NetBIOS name is written \\MYDOMAIN\SERVERA.

The On-line Help for Windows Server 2008 describes more about names in the sections DNS Domain Names and Name space planning for DNS.

Allocating 800xA Systems to Domains

All nodes in an 800xA System must be members of the same domain. A running 800xA System must always stay in the same domain. It is however possible to take a backup of a system and do the restore to another domain.

Several 800xA Systems may belong to the same domain. An 800xA System may belong to a domain which is also used for other types of systems. The 800xA System depends on the Domain Controller being available at all times. This means that it is important to consider if the availability of the Domain Controller will be sufficient if one domain is used for many types of systems.

When importing data with the import/export tool there are no restrictions regarding domain membership for the system that exported the data. It could belong to the same or a different domain or a workgroup.

When using Multisystem Integration the provider system and the subscriber system may belong to the same domain or to different domains, see [Multisystem Integration](#) on page 80.

Configuring Name Resolution and DNS

As soon as RNRP is correctly configured it will update the hosts files with addresses and names for the other nodes on the network. The host file service does not need any separate configuration in addition the normal RNRP configuration as described in [Section 2, Network Redundancy and Routing](#).

DNS configuration is done with the normal Windows configuration editors:

- For each node, including the DNS Servers:
Refer to [DNS Configuration in Each Node](#) on page 132.
 - Domain membership in the **System Properties**
 - Properties for each Network Interfaces for Network Areas where DNS is used
- In the DNS Server (refer to [DNS Server Configuration](#) on page 129):
 - Properties for the DNS server itself
 - Properties for the DNS Forward Lookup Zone
 - The records in the DNS Forward Lookup Zone

It is recommended to configure the DNS Server and to set up the DNS Forward Lookup Zone before anything else is done with the other nodes.

Which Nodes use host names

Client and Server functions in the System 800xA identify other nodes by their host names. This means that all **Clients and Servers must be known** by the DNS servers and by RNRP's host file service.

The applications in the AC 800M Controllers identify other nodes only by IP address and all Client and Server functions that communicate with the controllers also only identify the controllers by IP address.

This means that the **AC 800M Controllers will not be known** by the DNS servers or by RNRP's host file service.

Location of Domain Controllers



A Domain Controller and a DNS server are required to be on-line and operating to use the 800xA System. (unless a Workgroup is used)

The Domain Controller and the DNS server are installed on the same machine; the Domain Server. This should preferably be a dedicated node (or two for redundancy) that does not run any other 800xA System Software except RNRP (see [Configuring RNRP in a PC](#) on page 69). The main reason is that it simplifies the handling of backups and upgrades substantially, see [Backups of Domain Controllers](#) on page 126. It is however possible to combine the Domain Server and the Aspect Server in the same server node.

Maintaining Redundant Domain Controllers

DcDiag: Domain Controller Diagnostics

Microsoft provides a tool called DcDiag that can perform a number of tests of the health of a Domain Controller. DcDiag is included on the delivery of Windows Server 2008. It can also be downloaded from Microsoft's web site. `dcdiag /a` performs a test of all Domain Controllers in a site.



DcDiag will report an error if W32Time is disabled. Disregard this error message if you are using e.g. AfwTime instead of W32Time, see [Windows Time Service \(W32Time\)](#) on page 194.

Backups of Domain Controllers

It is possible to use image backups for redundant and non-redundant Domain Controllers. However, it is important not to exceed the Active Directory Tombstone Lifetime (by default 180 days in Windows Server 2008) when restoring a backup.



A backup which is older than the tombstone lifetime is normally not useful, unless all Domain Controllers are restored at the same time (with images taken not more than 180 days apart).

Microsoft Knowledge Base Article KB216993 describes more about this topic.

In addition to periodic complete backups of the Domain Controllers it is recommended to do a complete backup of the nodes just before they are promoted to become domains controller (dcpromo). This is a time when the active directory has not yet been created and this backup is therefore independent of the tombstone life time.

If a redundant Domain Controller fails it is possible to restore it from an image backup which was taken before promoting the server to become a Domain Controller. After restoring such a backup the content of the Active Directory must be replicated over from a Domain Controller which still is working properly.

Depending on what Domain Controller functions the lost server was responsible for some additional steps may need to be taken. So called FSMO roles may need to be seized by another Domain Controller and old stale FSMO records may need to be cleaned out. This process is described in the next section.

Recovering after a Crash of the First Installed Domain Controller

It is possible to use multiple Domain Controllers for a Domain. In most of their operation all Domain Controllers are equal but there are a number of roles that are only taken by the first PC that is promoted to be Domain Controller. The first installed Domain controller is by default the only one which is:

- FSMO role Schema Master
- FSMO role Domain Naming Master
- FSMO role PDC
- FSMO role RID master
- FSMO role Infrastructure master

If the first Domain Controller is permanently removed from the network there are some manual actions to do to make sure that the system keeps working in the long run. This involves the following steps:

1. Check if the removed server had the 5 FSMO roles
This is done with the tool **ntdsutil**. See below.
2. If necessary, seize the FSMO roles to one of the other servers
This is described in TechNet article KB255504

3. If there is no Global Catalog server: add a new Global Catalog. This is described in the TechNet article with the title “Add or Remove the Global Catalog“.
4. Remove the old server from the Active Directory This is described in TechNet article KB216498

To find out if the removed server had the 5 FSMO roles do the following at a command prompt:

```
ntdsutil: roles
fsmo maintenance: conn
server connections: conn to serv <a working server>
server connections: quit
fsmo maintenance: Select operation target
select operation target: list roles for conn ser
```

This gives the result:

```
Server <the working server> knows about 5 roles
Schema - CN=NTDS Settings,CN=<the removed server>,
CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=demo,DC=net
Domain - CN=NTDS Settings,CN=<the removed server>,
CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=demo,DC=net
PDC - CN=NTDS Settings,CN=<the removed server>,
CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=demo,DC=net
RID - CN=NTDS Settings,CN=<the removed server>,
CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=demo,DC=net
Infrastructure - CN=NTDS Settings,CN=<the removed server>,
CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=demo,DC=net
```


Time Synchronization in a Domain

The time must be synchronized between all nodes in a domain. The default setting is that if the time in a node differs more than 5 minutes compared to the Domain Controller the node is denied access to the domain. The limit is a parameter which is called the Kerberos Time Skew variable. See also [Windows Time Service \(W32Time\)](#) on page 194.

DNS Server Configuration

If more than one Domain Controller is used, you have to decide how they will be used as DNS Servers. Each node must be configured with one DNS Server as the **Preferred DNS Server**. Normally it is suggested to appoint one of the Domain Controllers to be the Primary DNS Server and configure **all nodes to use** it as the **Preferred DNS Server**. One reason is that this simplifies the replication between the DNS Servers. It is also easier to predict the behavior of the system if one of the Domain Controllers stops working. If the system is distributed so that different nodes are substantially closer to different Domain Controllers other configurations may be used.

The *System 800xA Installation (3BSE034679*)* manual describes how to set up a Domain Controller and DNS Server with DNS integrated in Active Directory. See also [Location of Domain Controllers](#) on page 126.

After the creation of the Domain Controller, make sure that the following is configured for DNS:

- The Computer Name tab (in **Start > Settings > Control Panel > System**) for the Domain Controller must indicate that it belongs to the newly created domain, see [Figure 49](#).
- The DNS server is running and there is a DNS Forward Lookup Zone for the network area(s) that will be used for Client Server communication. See [Figure 50](#) and [Figure 51](#). This typically means the Client Server Network but not the Control Networks or other extra networks, e.g. for backup handling or other management. The DNS Forward Lookup Zone will be populated with records for the clients and servers when they join the domain.

- The DNS Forward Lookup Zone is **Active Directory integrated** and allows dynamic update of records from nodes that enter the network, see [Figure 51](#). Make sure that the parameter **Dynamic updates** is set to **Secure Only**.
- In 800xA 5.1 no reverse lookup zones are necessary. The hosts file is used for both forward and reverse lookups.

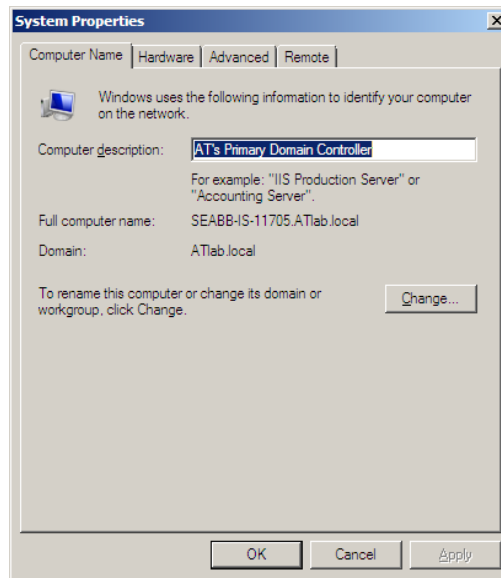


Figure 49. System Properties for a Domain Controller with Computer Name

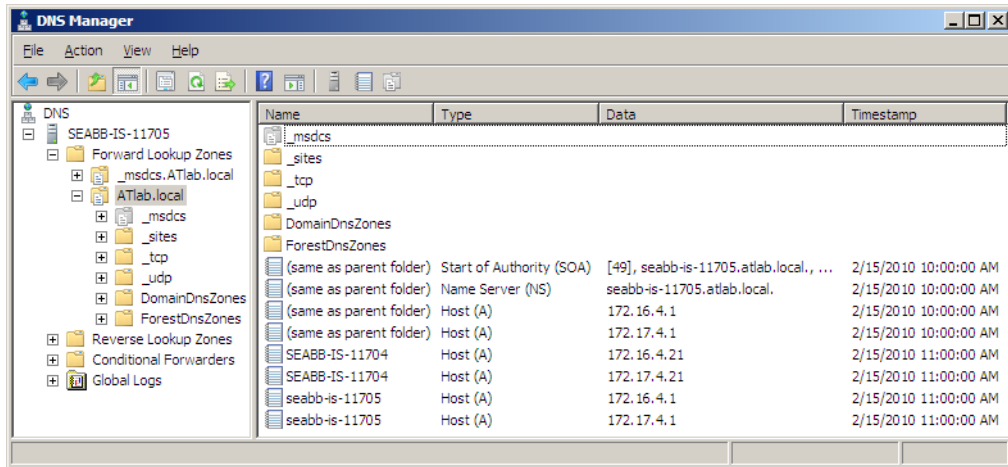


Figure 50. DNS entries for 800xA nodes. NB: Reverse lookup zones are not used

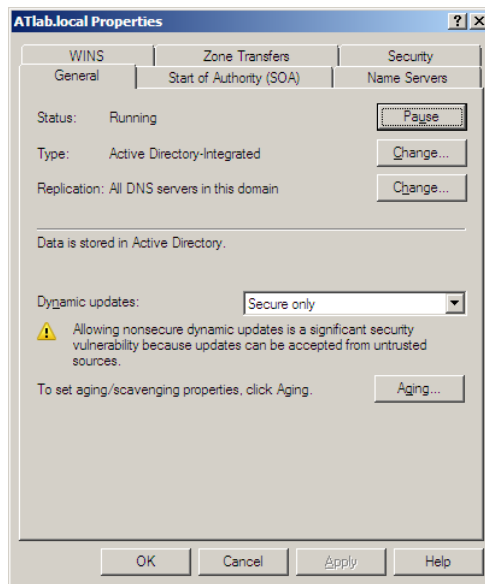


Figure 51. Properties for a DNS Forward Lookup Zone

Configuring a DNS Root Zone

For the normal case where an 800xA System is strictly local, i.e. no DNS queries are expected to be resolved by any external DNS server, it is recommended to configure a Root Zone (named “.”) in the DNS Servers. If a Root Zone is configured, a recursive query to other DNS servers is prohibited. If a Root Zone is not configured, a recursive query to other DNS servers will try to access all the default “Root Hints” servers, resulting in a long time out and final failure.

Only if a connection to an external Network, with an external DNS Server which shall be used, there shall be no Root Zone. In that case, the “Root Hints” Name servers shall be actualized.

DNS Configuration in Each Node

This section describes how to configure each node to fulfill the goals described in [Node name handling and DNS](#) on page 123, see [Figure 53](#).

General DNS configuration in each node

- The Primary DNS Suffix must be the same as the domain name. When joining the domain it will automatically be configured like this and normally does not need to be changed. To check that it is correct open **Start > Settings > Control Panel > System**, select the tab Computer Name, open Change and More, see [Figure 52](#).
- In all parameters where a DNS server is specified it shall be specified using its Primary Network Address.
- The DNS settings shall be the same for all Network interfaces, i.e. for Client Server Networks, Control Networks and any possible other network:
 - The Primary DNS Server shall be configured as the Preferred DNS Server.
 - The Secondary DNS server shall be configured as the Alternate DNS Server.
- The Primary Client Server Network shall be listed as the first interface.
- The parameter **Register this connection’s addresses in DNS** must be set for the Network Interfaces for network areas where DNS will be used. This is

typically **only the Client Server network**. This setting is required both for Domain based systems and systems using Workgroups.

- Use the default settings for NetBIOS for 800xA 5.1 and later.

See also [Verifying Name Resolution functions](#) on page 142.



Clients and servers shall be entered in the DNS Forward Lookup Zone. Controllers shall not be entered in the DNS Forward Lookup Zone. (See [Which Nodes use host names](#) on page 125)

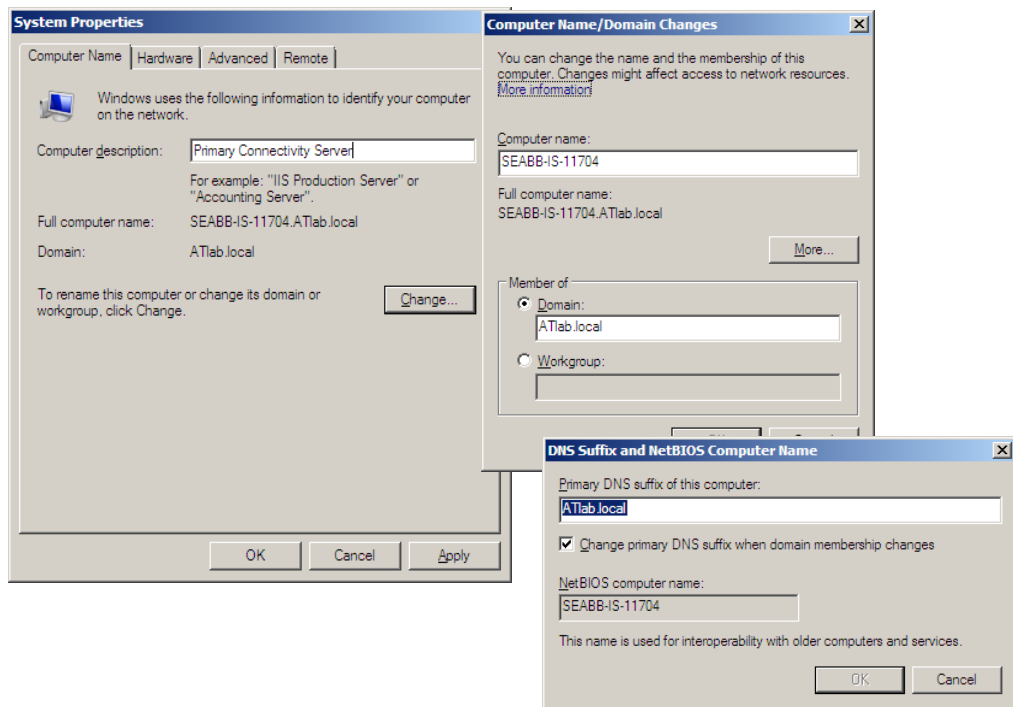


Figure 52. Full Computer Name and Primary DNS Suffix for Domain Member Computers

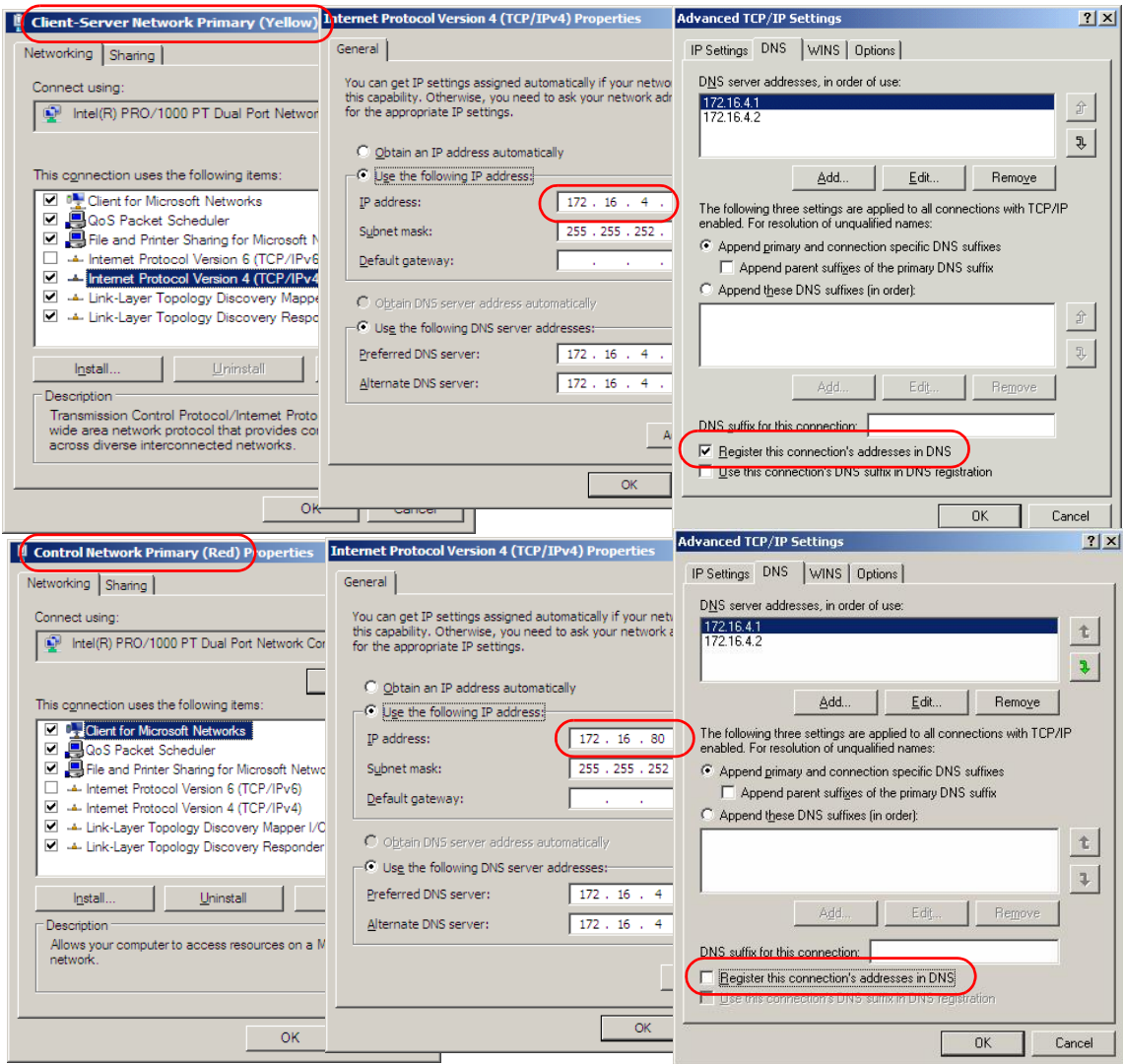


Figure 53. DNS Configuration for Client/Server and Control Network Interfaces
 NB! Only network areas using DNS shall be registered in DNS.

If the Domain Server uses any network interface in addition to the ones for the Client/Server Network the DNS server needs to be configured to only listen to DNS requests on the Client/Server network.

Open the **Interfaces** tab under Properties for the DNS Server and select **Only the following IP addresses** and ensure that only the IP addresses for the Clients/Server Network are checked, refer to [Figure 54](#). Do this for all Domain Servers.

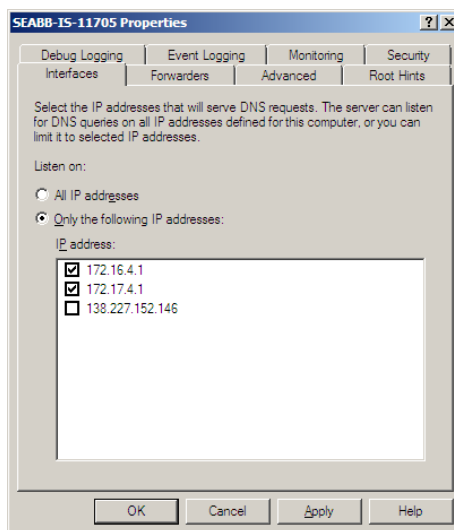


Figure 54. DNS Server Properties.

RNRP's host file service

As described in [Section 2, Network Redundancy and Routing](#), all nodes that use RNRP communicate with each other to exchange network status information. In System Version 5.1 RNRP also provides a service that exchanges information about host names. The information about the addresses and names of the nodes on the network is stored in the hosts file on each node.

RNRP creates host file entries for a network if it used by RNRP and the parameter **Register this connection's addresses in DNS** is checked for the primary path. The setting of this parameter for the secondary Network Interfaces does not matter.

This parameter shall be set only for networks on which Clients and Servers shall communicate, i.e. not for Control Networks or Ethernet based fieldbuses.

For redundant networks there will be host file entries for both paths. The entry for the primary path will be listed above the entry for the secondary path. This ensures that a forward lookup with a host name gives the primary address first.

RNRP's host file service automatically adds information about new nodes on the network. This means that in order to make a new node available to be added to the system the only actions a user needs to do is to set the IP addresses and make sure that RNRP is working on the node.

A DNS Server running Windows Server 2008 dynamically adds and removes host entries for nodes depending on with which addresses they are reachable. This is not acceptable in the 800xA System. One reason is that primary node addresses need to be known in the system even if only the secondary network is working.

For this reason RNRP does not automatically remove host file entries for nodes that are disconnected.

If you reconfigure or remove nodes so that information in the host file is no longer relevant you can manually refresh of the information in the host file. This is done with a button in the RNRP Wizard. After a question if refreshing the hosts file is indeed the desired action you can choose if the refresh shall be performed only on the local node or on all nodes on the network.

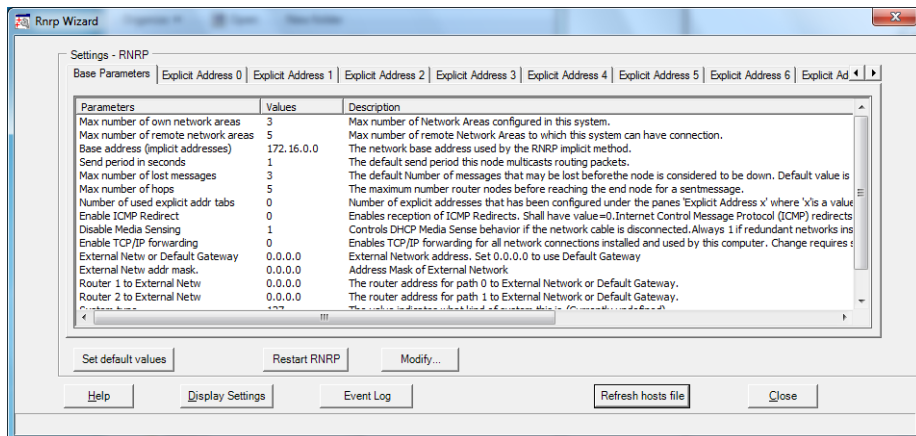


Figure 55. RNRP Wizard with button for Host File Refresh

If the host file is refreshed there will be an entry in the RNRP monitor:

```
15/2 *14:34:42.014 Hosts file refreshed by user
15/2 *14:34:48.659 Hosts file is Okey
```

The RNRP host file service updates a part of the hosts file that looks like this:

```
#BEGIN_800xA_RNRP
# Written by rnrp 2/10/2010

172.16.4.1 BCTID361.A1.local      # Area=1 Node=1 Path=0
172.17.4.1 BCTID361.A1.local      # Area=1 Node=1 Path=1
172.16.4.2 BCTID367.A1.local      # Area=1 Node=2 Path=0
172.17.4.2 BCTID367.A1.local      # Area=1 Node=2 Path=1
172.16.4.11BCTID221.A1.local     # Area=1 Node=11 Path=0
172.17.4.11BCTID221.A1.local     # Area=1 Node=11 Path=1
...
#END_800xA_RNRP
```



Do not edit the lines between the tags

#BEGIN_800xA_RNRP and #END_800xA_RNRP manually.

Lines before and after these tags may be edited manually if necessary but the tag #END_800xA_RNRP must always end with a CR (carriage return).

The RNRP monitor shows the node names for nodes where the RNRPs name resolution works as intended. See [Host names in the RNRP monitor](#) on page 238.

Configuring the Order of the Network Interfaces

To ensure that a node is always identified with its Primary IP address, it is important to set the order of the network interfaces correctly and not to change it; the primary network as the top selection, and the secondary network next.

For nodes that are connected to more than one network area the interfaces for the Client Server Network shall be listed before the interfaces for the Control Network¹. If any additional network interfaces are used these shall be listed after the ones for the Client Server Network and the Control Network.

1. Set the order in **Network Connections** in the **Network and Sharing Center** on each node.
2. Select **Advanced Settings** in the **Advanced** menu.

1. This is valid for Control Networks for all types of controllers, e.g. including Harmony, Melody, DCI controllers

3. Set the order of the Network Interfaces in the **Adapters and Bindings** tab, according to [Figure 56](#).

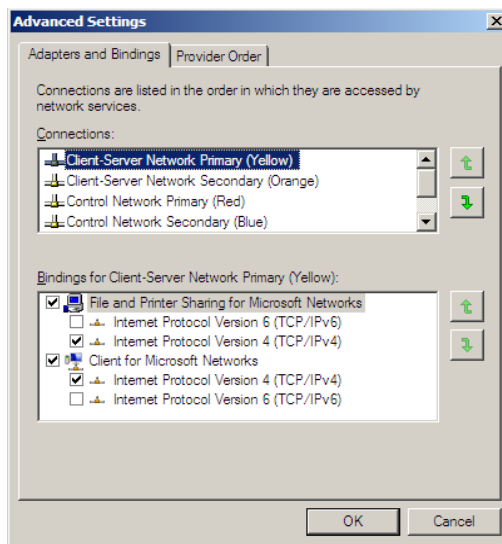


Figure 56. Network Interface Order

Windows Workgroups instead of Windows Domain

Small systems can run without a Domain Controller (and DNS server). In that case the PCs and users are not handled by a Windows Domain and instead a Windows Workgroup needs to be created.

A Windows Workgroup is not managed on a dedicated PC. The workgroup configuration needs to be done on all PCs that belong to the workgroup. This includes handling the names and addresses of the PCs and definition of users and groups. The handling of Users and groups in a Windows Workgroup is described in *System 800xA Administration and Security (3BSE037410*)*.

There is no fixed limit for the number of nodes or number of users that can be handled within a workgroup. Systems with more than 10 PCs or 5 users are normally easier to manage in a domain.



RNRP's Host file service works for both Domain based systems and systems using Workgroups. This means that from 800xA 5.1, no manual administration of host files is needed.

Note that the check box **Register this connection's addresses in DNS** must be checked for the Client Server Network.

Example of IP Addresses and DNS Configuration

This section describes an example of how to configure DNS for a system with the following features:

- Two Domain Controllers
- One Network Area for the Client Server Network
- Two Network Areas for Control Networks.
- One Control Network Area is handled by 2 Connectivity Servers
- One Controller with single CPU
- One Controller with redundant CPU

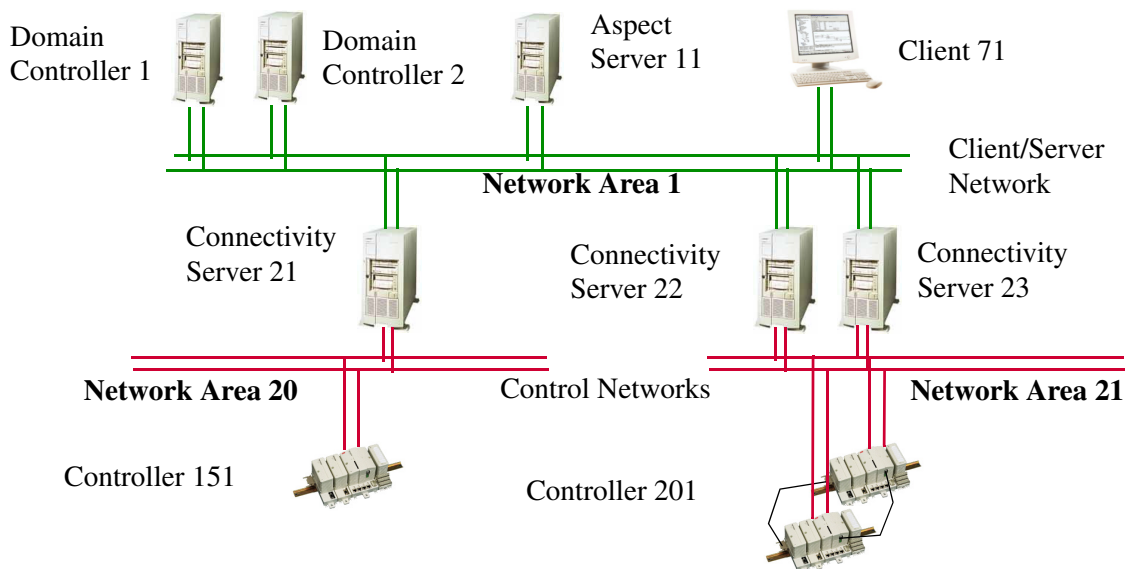


Figure 57. Example System to show DNS Configuration

This is not a recommended way to connect a system with only so few nodes. It is an example to show concepts. A system with more servers, clients and controllers would be configured in a similar way.

Table 12. DNS Configuration Example

Node name	Node	Area	Path	IP Address	Preferred DNS server	Alternate DNS server	Auto register in DNS
Domain Controller 1	1	1	0	172.16.4.1	172.16.4.1	172.16.4.2	Yes
			1	172.17.4.1	172.16.4.1	172.16.4.2	Yes
Domain Controller 2	2	1	0	172.16.4.2	172.16.4.1	172.16.4.2	Yes
			1	172.17.4.2	172.16.4.1	172.16.4.2	Yes
Aspect Server 11	11	1	0	172.16.4.11	172.16.4.1	172.16.4.2	Yes
			1	172.17.4.11	172.16.4.1	172.16.4.2	Yes

Table 12. DNS Configuration Example

Node name	Node	Area	Path	IP Address	Preferred DNS server	Alternate DNS server	Auto register in DNS
Connectivity Server AC 800M 21	21	1	0	172.16.4.21	172.16.4.1	172.16.4.2	Yes
			1	172.17.4.21	172.16.4.1	172.16.4.2	Yes
	20	0	172.16.80.21	172.16.4.1	172.16.4.2	No	
		1	172.17.80.21	172.16.4.1	172.16.4.2	No	
Connectivity Server AC 800M 22	22	1	0	172.16.4.22	172.16.4.1	172.16.4.2	Yes
			1	172.17.4.22	172.16.4.1	172.16.4.2	Yes
	21	0	172.16.84.22	172.16.4.1	172.16.4.2	No	
		1	172.17.84.22	172.16.4.1	172.16.4.2	No	
Connectivity Server AC 800M 23	23	1	0	172.16.4.23	172.16.4.1	172.16.4.2	Yes
			1	172.17.4.23	172.16.4.1	172.16.4.2	Yes
	21	0	172.16.84.23	172.16.4.1	172.16.4.2	No	
		1	172.17.84.23	172.16.4.1	172.16.4.2	No	
Client 71	71	1	0	172.16.4.71	172.16.4.1	172.16.4.2	Yes
			1	172.17.4.71	172.16.4.1	172.16.4.2	Yes
Controller 151 Single CPU	151	20	0	172.16.80.151	[n.a.]	[n.a.]	[n.a.]
			1	172.17.80.151	[n.a.]	[n.a.]	[n.a.]
Controller 201 Redundant CPU	201	21	0	172.16.84.201	[n.a.]	[n.a.]	[n.a.]
			1	172.17.84.201	[n.a.]	[n.a.]	[n.a.]
Backup CPU			0	172.16.86.201	[n.a.]	[n.a.]	[n.a.]
			1	172.17.86.201	[n.a.]	[n.a.]	[n.a.]

Table 12 shows how to set the DNS parameters for the Network Adapters in the PCs and what IP addresses to have in the DNS Forward Lookup Zone.

Each row in Table 12 represents a network interface in a PC or a Controller.

Node, Area and Path are the RNRP address parameters for the Network Interface.

[n.a.] means “not applicable”, e.g. the parameter Preferred DNS server does not exist for the network interfaces in the controllers.

“Auto register in DNS” Yes/No tells if the check box “Register this connections addresses in DNS” is to be marked or not.

Use the default setting for NetBIOS.

Verifying Name Resolution functions

The RNRP monitor shows node names

The RNRP monitor shows the node names for nodes where the RNRP’s host file service works as intended. See [Host names in the RNRP monitor](#) on page 238.

ping -a instead of nslookup

The command line utility **ping** with the option **-a** provides a way to find out if a node resolves names properly.

ping -a can provide both forward lookup (address resolution)

```
C:\Users\Administrator>ping -a SEABB-IS-11704.ATlab.local
```

```
Pinging SEABB-IS-11704.ATlab.local [172.16.4.21] with 32 bytes of data:  
...
```

and reverse lookup (name resolution).

```
C:\Users\Administrator>ping -a 172.16.4.21
```

```
Pinging SEABB-IS-11704.ATlab.local [172.16.4.21] with 32 bytes of data:  
...
```

The name and address information is displayed independent of if the node actually responds to the ping requests.

When using host files for name resolution **nslookup** is not a good tool to analyze name resolution problems since nslookup only uses DNS. It does not use the information in the host file.

Special Considerations when Changing DNS Configuration

When changing the DNS configuration pay special attention to when the changes are actually applied.

If the IP address of a node is changed the DNS Server is not immediately notified. Notification normally occurs at startup of the node. To force notification, use the

command line utility `ipconfig /registerdns` in a command window on the node that will be registered.

When a node makes a DNS query the response is stored in a local cache to speed up subsequent queries. This implies that changes in the DNS server are not immediately noticed in client nodes. To empty the local DNS cache use the command line utility `ipconfig /flushdns` in a command window on the node that is to be refreshed.

If the two DNS Servers give different responses the replication between the DNS Servers may not have been completed since the last change. Read more in the On-line help on the Windows Server 2008 about replication of Active Directory.

Section 7 Time Synchronization

This section describes how to synchronize real time clocks in an 800xA System.

The first part of the section describes recommended time synchronization schemes for the most common configurations:

1. [Local Time Source](#) on page 146.
2. [External Time Source](#) on page 150.
3. [Windows Time Instead of AfwTime](#) on page 153.
4. [Systems with More Than One Control Network](#) on page 156.
5. [Time Synchronization with Multisystem Integration](#) on page 157.
6. [Systems with MB 300 and 800xA for AC 800M](#) on page 160
7. [MB 300 as Time Source for AC 800M](#) on page 164.
8. [Synchronization from the Client Server Network](#) on page 167.

This is followed by a section describing how to set different configuration parameters in controllers:

- [Configure Time Synchronization in Controllers](#) on page 171.

The rest of this section describes the different protocols and time synchronization components:

- [CNCN - Control Network Clock Protocol](#) on page 174.
- [SNTP - Simple Network Time Protocol](#) on page 176.
- [MB 300 Time Synchronization](#) on page 178.
- [MMS Time Synchronization](#) on page 180.
- [AfwTime Service](#) on page 180.
- [Time Synchronization for Connectivity Servers, Time Adaptors](#) on page 188.
- [Windows Time Service \(W32Time\)](#) on page 194.

Recommended Time Synchronization Schemes

To achieve the best time accuracy in the total system, it is recommended to distribute the time “upwards” in the system, from the Control Network to the Client Server Network. Typically a controller will act as time master for the Control Network and the rest of the system will be synchronized from this source.

This way of synchronizing is better than the other direction, because the protocols on the Control Network support a higher accuracy and the implementations of the real-time clocks in the Controllers are better than the protocols used between PCs and the Windows time.

The time source can be a Controller (see [Local Time Source](#) on page 146) or an external time source (see [External Time Source](#) on page 150).

Use an external time source if it is important that time stamps in the system are possible to compare with time stamps from other systems.



The following sections describe some different alternatives for Time Synchronization including tables with recommended settings. Where and how the settings are done is described in the protocol sections (CNCP, SNTP, AfwTime, Windows Time Service etc.) later in this chapter.

Local Time Source

If it is not important that the clocks in the system are well synchronized with clocks in the rest of the world, it is sufficient to let one (or more to get redundancy) of the controllers act as the time source for the whole system. When using AC 800M controllers CNCP is the recommended protocol for time synchronization to all nodes on the Control Network that support CNCP. This includes all 800xA PCs that are connected to the Control Network and use 800xA for AC 800M. If the Control Network is separated from the Client Server Network, normally only the AC 800M connectivity servers are connected directly to the Control Network. These PCs shall use the option, AC 800M Time Adaptor, to act as CNCP time slaves and should also run the AfwTime Server. The other PCs shall run the AfwTime Client.

Let the Domain Controllers fetch the time from time source controller using SNTP. If they are not connected to the same network area as the controller, TCP/IP forwarding must be enabled in the connectivity server (see [Table 5](#) in section [RNRP Configuration Parameters](#) on page 54).

When using 800xA for Harmony, 800xA for Melody, or 800xA for Advant Master the connectivity servers shall act as SNTP server for the Domain Controller, see for example [MB 300 as Time Source for AC 800M](#) on page 164.

When using a local time source it is recommended to periodically check and possibly adjust the system time manually, e.g. once or a few times per year. To be able to do this the controllers must be set to accept manual time setting. This is done by setting the parameter “CS Time Set Enable” = true. See also section [Setting the System Time](#) on page 199.

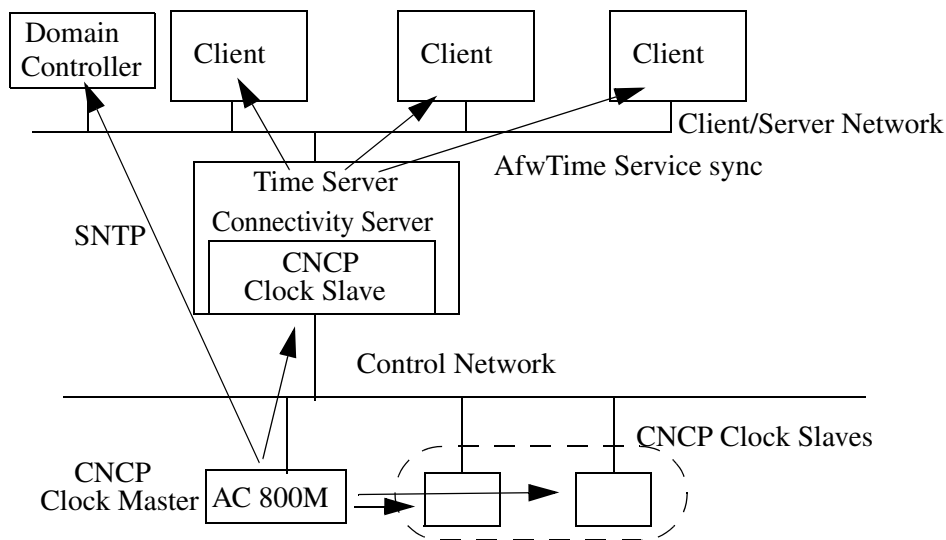


Figure 58. Time Synchronization with Local Time Source

Configuration of the Different Nodes

Table 13. Time Sync Configuration in Controllers: Local Time Source

	Controller Type		
	Up to 10 AC 800Ms	Up to 9 AC 800Ms	Other Controllers
Time Sync Protocol, Role	CNCP, Master SNTP Server	CNCP, Master SNTP Server	CNCP, Slave
Parameters			
CS CNCP Clock Master Order Number	1	2,3...10	0
CS Protocol Type	No Synch	CNCP	CNCP
CS Time Set Enabled	True	True	True
CS Synchronization Interval	20	20	<don't care>
CS SNTP Server Addr 1	<empty>	<empty>	<empty>
CS SNTP Server Addr 2	<empty>	<empty>	<empty>

Table 14. Configuration of the AfwTime Service: Local Time Source

Parameters	Value
Server Running	True
Clients Allowed to set time	False
Synchronization Interval (sec.)	20

Table 15. Time Sync Configuration in Clients and Servers: Local Time Source

		Node Type	
		Connectivity Servers	Other 800xA System Nodes
CNCP Role		Slave	<not used>
AC 800M Time Adaptor		Installed	Not installed
Other Time Adaptors		Not installed	Not installed
AfwTime Service Role		Server	Client
Time Service Provider Definition	Enabled	True	False
TimeServerHandler	Time Synchronization Running	True	True
	Allowed to set time	False	False
W32Time	Startup type	Disabled	Disabled

Table 16. Time Sync Configuration in Dedicated Domain Controller:
Local Time Source

SNTP Server addresses		w32tm /config /manualpeerlist:"A.B.C.D A.B.E.F" (the addresses of the Controllers that act as SNTP Servers)
W32Time service	Startup type	Automatic
	Server status	Started
Windows Registry parameters for W32Time	NtpServer	Enabled = 0
	NtpClient	Enabled = 1
	Type	NTP (this is set by w32tm /config /manualpeerlist)

External Time Source

If the system needs to be synchronized with a global time master, the recommended method is to use an SNTP server with a GPS receiver.

Connect the SNTP server to the Control Network and configure all AC 800M controllers to fetch the time via SNTP.

Configure two AC 800M as CNCP Clock Masters to synchronize the connectivity servers as in the case with Local Time Source. It is possible to use only a few controllers as SNTP clients and let the others be CNCP slaves.

The best over all accuracy is achieved with one or more High Precision SNTP Servers connected to each network area. Use at least two servers to improve the availability. Since these products do not support RNRP one of them shall be connected to the primary network and the other to the secondary network.

Dedicated Domain Controllers may also synchronize directly from the SNTP servers. For this traffic to find its way TCP/IP forwarding must be enabled in the connectivity servers and the SNTP servers need to have the “Default Gateway” parameter set to the address of a Connectivity Server.

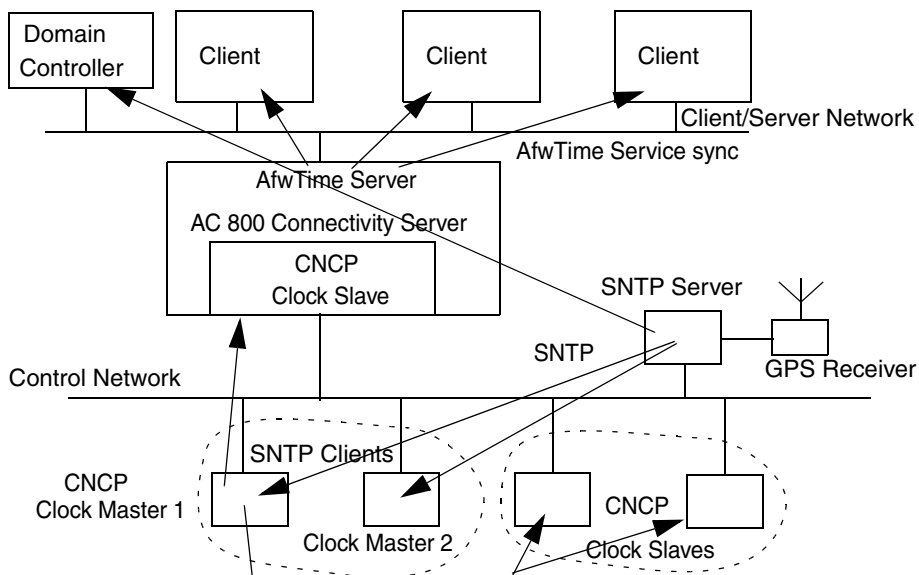


Figure 59. Using an External Time Source

Configuration of the Different Nodes

Table 17. Time Sync Configuration in Controllers: External Time Source

	Controller Type	
	2 Controllers	Other Controllers
Time Sync Protocol, Role	SNTP, Client CNCP, Master	CNCP, Slave
Parameters		
CS CNCP Clock Master Order Number	1,2	0
CS Protocol Type	SNTP	CNCP
CS Time Set Enabled	False	False
CS Synchronization Interval	20	<don't care>
CS SNTP Server Addr 1	A.B.C.D	<empty>
CS SNTP Server Addr 2	A.E.F.G	<empty>

A.B.C.D and A.E.F.G are the addresses of the SNTP servers. One on each network path.

Table 18. Configuration of the AFWTime Service: External Time Source

Parameters	Value
Server Running	True
Clients Allowed to set time	False
Synchronization Interval (sec.)	20

Table 19. Time Sync Configuration in Clients and Servers: External Time Source

		Node Type	
		Connectivity Servers	Other 800xA System Nodes
CNCP Role		Slave	<not used>
AC 800M Time Adaptor		Installed	Not installed
Other Time Adaptors		Not installed	Not installed
AfwTime Service Role		Server	Client
Time Service Provider Definition	Enabled	True	False
TimeServerHandler	Time Synchronization Running	True	True
	Allowed to set time	False	False
W32Time	Startup type	Disabled	Disabled

Table 20. Time Sync Configuration in Dedicated Domain Controller: External Time Source

SNTP Server addresses		w32tm /config /manualpeerlist:"A.B.C.D A.B.E.F" (the addresses of the external SNTP Servers)
W32Time service	Startup type	Automatic
	Server status	Started
Windows Registry parameters for W32Time	NtpServer	Enabled = 0
	NtpClient	Enabled = 1
	Type	NTP (this is set by w32tm /config /manualpeerlist)

Windows Time Instead of AfwTime

If it is not important to have a high time synchronization accuracy in the system it is possible to use the standard settings of Windows Time to synchronize the PCs. This means that all PCs will fetch the time from the Domain Controller.

It is still a good idea to use a controller or even an external SNTP server as time source for the system but the AfwTime service is not needed and must be disabled.

By tuning NTP parameters in the Windows Registry it is possible to achieve a quite good time synchronization accuracy also with this method. This however gives a configuration which is a bit tricky to maintain.

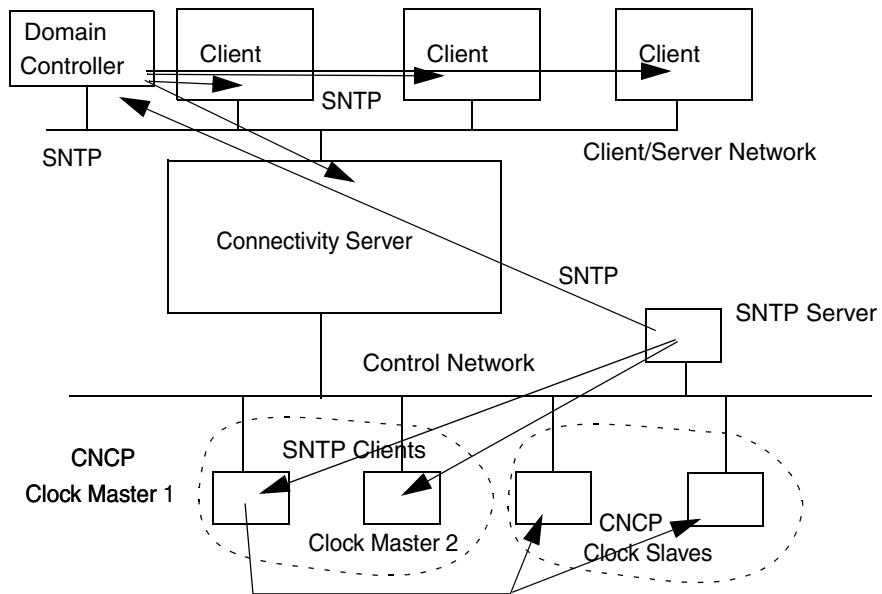


Figure 60. Using Windows Time to synchronize the PCs

Configuration of the Different Nodes

Table 21. Time Sync Configuration in Controllers: Windows Time Sync

	Controller Type		
	2 AC 800Ms	Other AC 800Ms	Other Controllers
Time Sync Protocol, Role	SNTP, Client CNCP, Master	SNTP, Client	CNCP, Slave
Parameters			
CS CNCP Clock Master Order Number	1,2	0	0
CS Protocol Type	SNTP	SNTP	CNCP
CS Time Set Enabled	False	False	False
CS Synchronization Interval	20	20	<don't care>
CS SNTP Server Addr 1	A.B.C.D	A.B.C.D	<empty>
CS SNTP Server Addr 2	A.E.F.G	A.E.F.G	<empty>

A.B.C.D and A.E.F.G are the addresses of the SNTP servers. One on each network path.

Table 22. Configuration of the AfwTime Service: Windows Time sync

Parameters	Value
Server Running	False
Clients Allowed to set time	False
Synchronization Interval (sec.)	<don't care>

Table 23. Time Sync Configuration in Clients and Servers: Windows Time Sync

		Node Type	
		Connectivity Servers	Other 800xA System Nodes
CNCP Role		<not used>	<not used>
Time Adaptors		Not installed	Not installed
AfwTime Service Role		<not used>	<not used>
Time Service Provider Definition	Enabled	False	False
TimeServerHandler	Time Synchronization Running	False	False
	Allowed to set time	False	False
SNTP Role		Client	Client
W32Time	Startup type	Enabled	Enabled
	Server status	Started	Started

Table 24. Time Sync Configuration in Dedicated Domain Controller: Windows Time sync

SNTP Server addresses		w32tm /config /manualpeerlist:"A.B.C.D A.B.E.F" (the addresses of the external SNTP Servers)
W32Time service	Startup type	Automatic
	Server status	Started
Windows Registry parameters for W32Time	NtpServer	Enabled = 1
	NtpClient	Enabled = 1
	Type	NTP (this is set by w32tm /config /manualpeerlist)

Systems with More Than One Control Network

If a system contains connectivity servers for more than one Control Network, the best system wide time synchronization accuracy is achieved by using externally synchronized time sources, for example (S)NTP time servers with GPS receivers. The connectivity server(s) for one of the Control Networks must be responsible for synchronizing the Client/Server Network. Delete the AfwTime Server in the other Connectivity servers (see [Figure 77 on page 185](#))

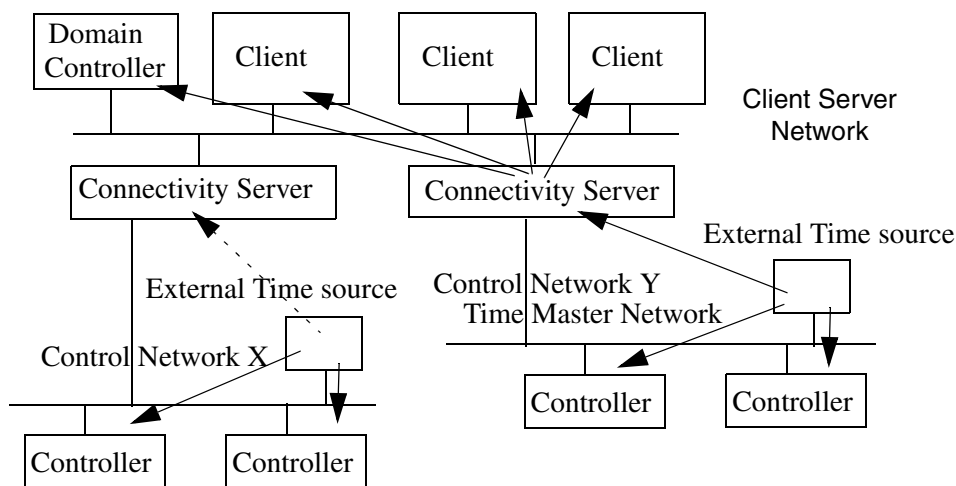


Figure 61. Time Synchronization with more than one Control Network

To reduce the number of time servers it is possible to let controllers in one Control Network use time servers in another Control Network via routing through the Connectivity Servers. This gives a lower synchronization accuracy than if only local servers are used, but with AC 800M controllers synchronizing from good SNTP servers it can still be better than 1 ms between all controllers in the system.

Time Synchronization configuration in the Connectivity Servers differ between the different Connect Products:

For 800xA for AC 800M see [AC 800M Time Adaptor](#) on page 189.

For 800xA for Advant Master see [Advant Master Time Adaptor](#) on page 189.

For 800xA for Harmony see [Time Sync with 800xA for Harmony](#) on page 192.

For 800xA for Melody see [Time Sync with 800xA for Melody](#) on page 193.

Time Synchronization in the Control Networks that are not acting as time sources for the Client/Server network also differs between Controller families:

- 800xA for AC 800M, 800xA for Harmony and 800xA for Melody: Use a GPS clock or similar.
- 800xA for Advant Master: Connect the MB 300 network with an AC 800M controller with CI855, see [Systems with MB 300 and 800xA for AC 800M](#) on page 160.
It is possible but not recommended to let the Advant Master Connectivity server synchronize the MB 300 network, see [Reverse Synchronization Mode](#) on page 190.

The Connectivity Servers for these Control Networks may be synchronized from their own Control Networks or the same way as the rest of the nodes on the Client Server Network.

Time Synchronization with Multisystem Integration

In an automation system consisting of more than one 800xA System (see [Multisystem Integration](#) on page 80) there are some things to pay special attention to when planning the time synchronization:

- The clocks in the different 800xA Systems should be synchronized. If the clocks differ more than 5 minutes between the provider system and the subscriber system a system event will be generated in the subscriber system once per hour.
- AfwTime can only distribute time to nodes belonging to the same 800xA System (same Aspect Directory). None of the other synchronization protocols have any notion of the Aspect Directory:
 - A CNCP master synchronizes all CNCP slaves on the same network area independent of which 800xA System the nodes belong to.
 - An SNTP server can be used by SNTP clients independent of which 800xA System the nodes belong to.

The following sections describe some different alternatives for a system with Multisystem Integration.

Different Systems on the Same Control Network

If there is a Control Network that all systems are connected to let one AC 800M controller be CNCP master and receive the time in the connectivity servers for the different systems with the 800xA for AC 800M Time Adaptor. The configuration will be similar to [Local Time Source](#) on page 146. SNTP with high accuracy may also be used as in [Windows Time Instead of AfwTime](#) on page 153.

Different Systems on Different Networks

If the systems are not connected via the Control Network the best accuracy is achieved using an external time source in each system as in [Systems with More Than One Control Network](#) on page 156, see [Figure 62](#).

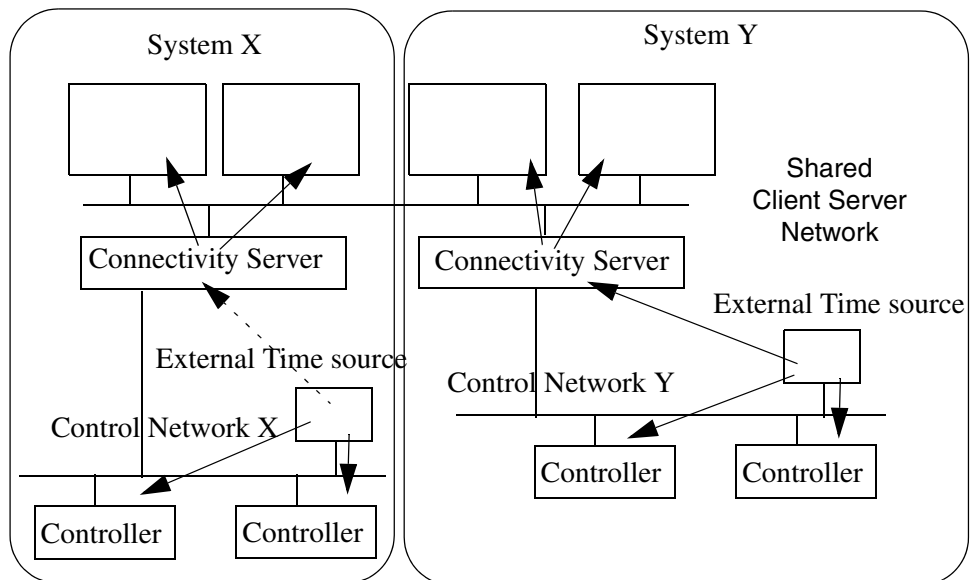


Figure 62. Time Synchronization of Multisystem Integration with External Time Sources

Different Systems on Connected Networks

If the accuracy requirement is not so high let one (or two for redundancy) node in one system be SNTP server for nodes in other systems.

If the networks in all systems are connected as one RNRP network all nodes in all systems may reach each other with routing. This can be used so that one controller in the provider system is SNTP server for a controller in the subscriber system which is SNTP client. That controller may then distribute the time with e.g. CNCP upwards in its system, see [Figure 63](#).

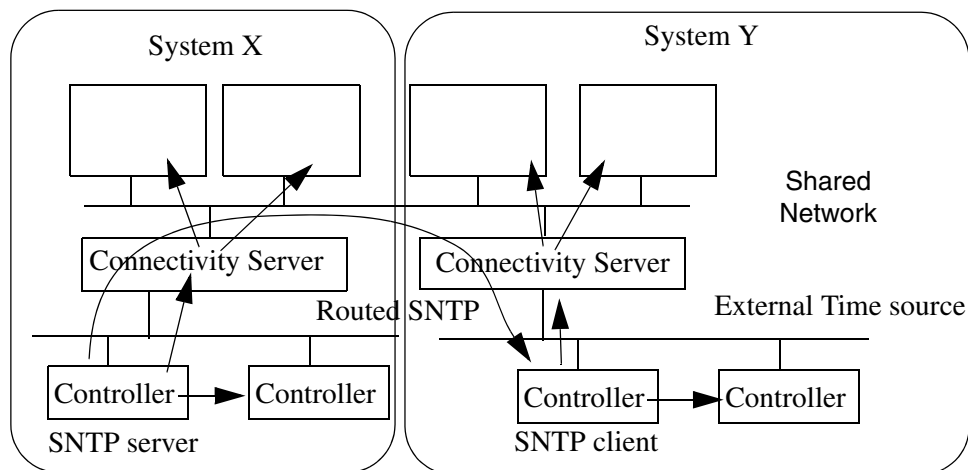


Figure 63. Time Synchronization of Multisystem Integration with Routed SNTP

Another method is to use the node that runs the Remote Access Server as SNTP server and the node that runs the Remote Access Client as SNTP client. The rest of the nodes on the Client Server Network may be synchronized with the AfwTime service, see [Figure 64](#). Since this involves using one or more PCs as SNTP servers (according to [Enable the SNTP Server, Disable SNTP Client in a PC](#) on page 196) this will however probably be more difficult to configure than the alternative in [Figure 63](#).

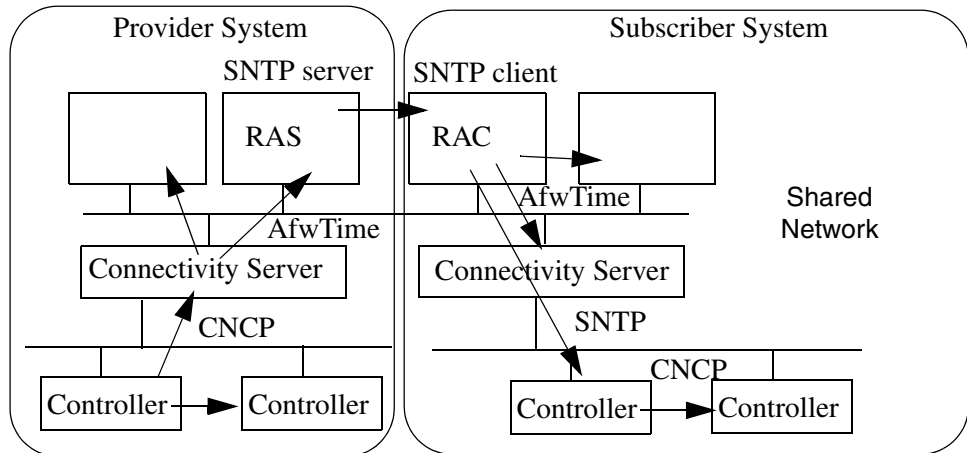


Figure 64. Time Synchronization of Multisystem Integration with SNTP from the RAS node to the RAC node

Systems with MB 300 and 800xA for AC 800M

If a system contains both a MB 300 network and a Control network with AC 800M Controllers, it is recommended to use a CI855 in at least one AC 800M so that the time can be distributed from the Control Network to MB 300 via CI855. The following description is based on an AC 800M being the time source for the entire system.

If an external SNTP server is used, the AC 800M controllers must be configured as in [Windows Time Instead of AfwTime](#) on page 153. The other nodes will be configured in the same way as described below.

In this example the AfwTime Service is used on the Client Server Network, but the W32Time service may be used as in [Local Time Source](#) on page 146.

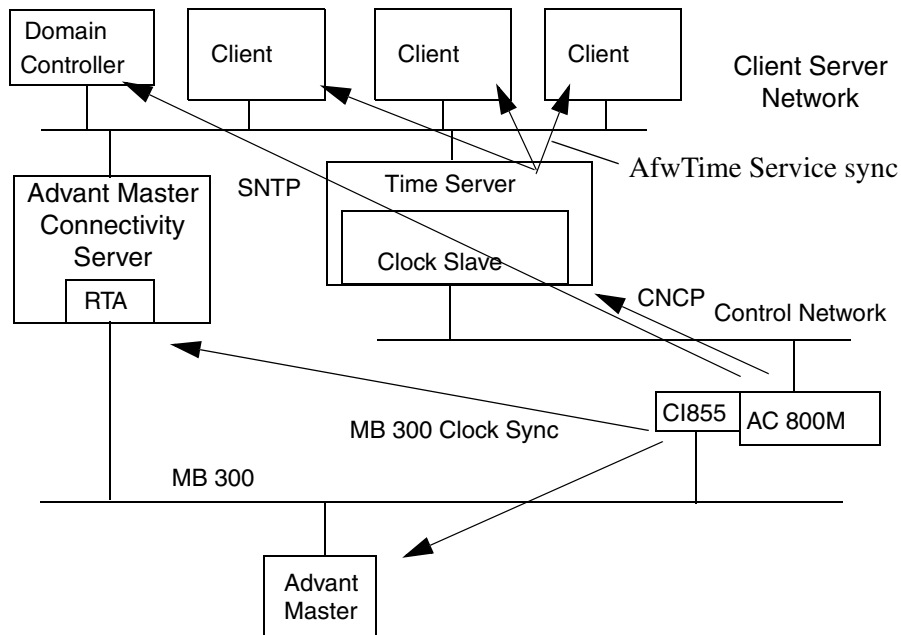


Figure 65. Time Synchronization with Both MB 300 and the Control Network

Configuration of the Different Nodes

Table 25. Time Sync Configuration in Controllers: AC 800M to MB 300

	Controller Type	
	One or two AC 800Ms	Other Controllers
Time Sync Protocol, Role	CNCP, Master MB 300, Master	CNCP, Slave
Parameters		
CS CNCP Clock Master Order Number	1,2	0
CS Protocol Type	CNCP (don't care)	CNCP

Table 25. Time Sync Configuration in Controllers: AC 800M to MB 300

	Controller Type	
	One or two AC 800Ms	Other Controllers
CS Time Set Enabled	True	True
CS Synchronization Interval	20	<don't care>
CS SNTP Server Addr 1	<empty>	<empty>
CS SNTP Server Addr 2	<empty>	<empty>
Configuration for CI855: Time Synchronization	MB 300 Master	<not used>

Table 26. Configuration of the AfwTime Service: AC 800M to MB 300

Parameters	Value
Server Running	True
Clients Allowed to set time	False
Synchronization Interval (sec.)	20

*Table 27. Time Sync Configuration in Advant Master Controllers on MB 300:
AC 800M to MB 300*

Parameters on the Clock Synch DB element	Value
CLK_MAST	0
LOC_TIME	2
CLK_SEND	0

Table 28. Time Sync Configuration in Clients and Servers: AC 800M to MB 300

		Node Type		
		AC800M Connectivity Servers	Advant Master Connectivity Servers	Other 800xA System Nodes
CNCP Role		Slave	<not used>	<not used>
AC 800M Time Adaptor		Installed	Not installed	Not installed
Other Time Adaptors		Not installed	Not installed	Not installed
AfwTime Service Role		Server	Client	Client
Time Service Provider Definition	Enabled	True	False	False
TimeServerHandler	Time Synchronization Running	True	True	True
	Allowed to set time	False	False	False
MB 300 Clock Synch Role		<not used>	Slave	<not used>
MB 300 Clock Sync Config for the Clock Synch DB element on the RTA board	CLK_MAST	<not used>	0	<not used>
	LOC_TIME	<not used>	2	<not used>
	CLK_SEND	<not used>	0	<not used>
W32Time	Startup type	Disabled	Disabled	Disabled

Table 29. Time Sync Configuration in Dedicated Domain Controller: AC 800M to MB 300

SNTP Server addresses		w32tm /config /manualpeerlist:"A.B.C.D A.B.E.F" (the addresses of the Controllers that act as SNTP Servers)
W32Time service	Startup type	Automatic
	Server status	Started
Windows Registry parameters for W32Time	NtpServer	Enabled = 0
	NtpClient	Enabled = 1
	Type	NTP (this is set by w32tm /config /manualpeerlist)

MB 300 as Time Source for AC 800M

For existing systems with Advant Master that are extended with 800xA for AC 800M it is often a requirement to synchronize the new AC 800M controllers from the Advant Master Controllers via the CI855. This is also possible.

A draw back (compared to the previous alternative) is that the MB 300 time sync protocol uses local time and the Advant Master Controllers do not handle Daylight Savings Time changes. The Advant Master Controller which is time sync master appoints a RTA board or a CI855 to handle the shifting of Daylight Savings Time.

The following description is based on an AC 400 controller being the time source for the entire system. That controller may additionally be synchronized with a minute pulse.

In this type of configuration it is recommended to use AfwTime Service on all 800xA nodes in the Client Server Network. It is necessary at least for the Advant Master Time Adaptor.

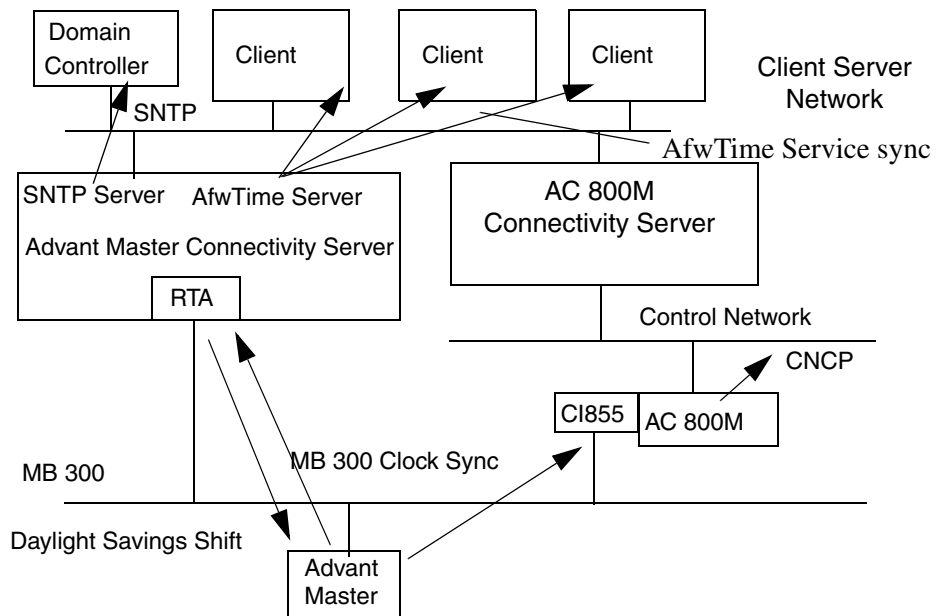


Figure 66. Time Synchronization with Both MB 300 and the Control Network

Configuration of the Different Nodes

Table 30. Configuration in Clock Sync Master on MB 300: only MB 300

Parameters on the Clock Synch DB element	Value
CLK_MAST	1
LOC_TIME	2
CLK_SEND	1

Table 31. Time Sync Configuration in AC 800M Controllers: MB 300 to AC 800M

	Controller Type	
	AC 800Ms connected to MB 300	Other Controllers
Time Sync Protocol, Role	CNCP, Master MB 300, slave	CNCP, Slave
Parameters		
CS CNCP Clock Master Order Number	1,2	0
CS Protocol Type	MB 300	CNCP
CS Time Set Enabled	False	False
CS Synchronization Interval	20	<don't care>
CS SNTP Server Addr 1	<empty>	<empty>
CS SNTP Server Addr 2	<empty>	<empty>
Configuration for CI855: Time Synchronization	MB 300 Slave	<not used>

Table 32. Configuration of the AfwTime Service: MB 300 to AC 800M

Parameters	Value
Server Running	True
Clients Allowed to set time	False
Synchronization Interval (sec.)	20

Table 33. Time Sync Configuration in Clients and Servers: MB 300 to AC 800M

		Node Type	
		Advant Master Connectivity Servers	Other 800xA System Nodes
Advant Master Time Adaptor		Installed	Not installed
Other Time Adaptors		Not installed	Not installed
AfwTime Service Role		Server	Client
Time Service Provider Definition	Enabled	True	False
TimeServerHandler	Time Synchronization Running	True	True
	Allowed to set time	False	False
MB 300 Clock Synch Role		Slave, DST Master	<not used>
MB 300 Clock Sync Config for the Clock Synch DB element on the RTA board	CLK_MAST	0	<not used>
	LOC_TIME	2	<not used>
	CLK_SEND	1	<not used>
SNTP role		Server	<not used>
W32Time	Startup type	Automatic	Disabled
	Server status	Started	Stopped
SNTP parameters in Windows Registry	NtpServer	Enabled = 1	<don't care>
	NtpClient	Enabled = 0	<don't care>
	Type	NoSync	<don't care>

Table 34. Time Sync Configuration in Domain Controller: MB 300 to AC 800M

SNTP Server addresses		w32tm /config /manualpeerlist:"A.B.C.D A.B.E.F" (the addresses of the Advant Master Connectivity Servers that act as SNTP Servers)
W32Time service	Startup type	Automatic
	Server status	Started
Windows Registry parameters for W32Time	NtpServer	Enabled = 0
	NtpClient	Enabled = 1
	Type	NTP (this is set by w32tm /config /manualpeerlist)

Synchronization from the Client Server Network

With 800xA for AC 800M and 800xA for Advant Master it is possible to synchronize the clocks in the controllers from the Client Server network through the connectivity servers. This is normally not the recommended solution. It typically gives lower accuracy of the clocks in the controllers. In this example the Domain Controller is synchronized by an external SNTP server.

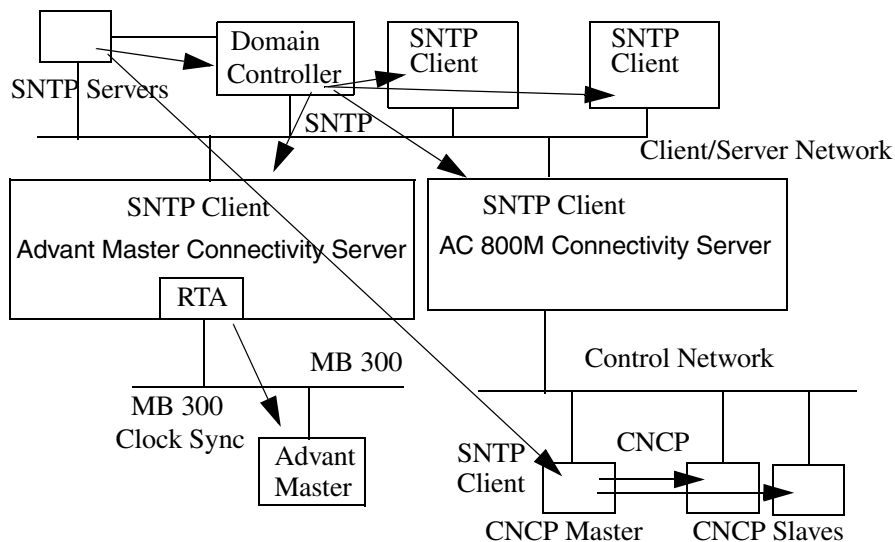


Figure 67. Synchronizing from the Client Server Network

Configuration of the Different Nodes

Table 35. Time Sync Configuration in Controllers: Reversed Sync

	Controller Type	
	2 AC 800Ms	Other Controllers
Time Sync Protocol, Role	SNTP, Client CNCP, Master	CNCP, Slave
Parameters		
CS CNCP Clock Master Order Number	1,2	0
CS Protocol Type	SNTP	CNCP
CS Time Set Enabled	False	False
CS Synchronization Interval	20	<don't care>
CS SNTP Server Addr 1	A.B.C.D	<empty>
CS SNTP Server Addr 2	A.E.F.G	<empty>

Table 36. Time Sync Configuration in Advant Master Controllers on MB 300: Reversed Sync

Parameters on the Clock Synch DB element	Value
CLK_MAST	0
LOC_TIME	2
CLK_SEND	0

A.B.C.D and A.E.F.G are the addresses of the external SNTP servers. One on each network path.

Table 37. Configuration of the AfwTime Service: Reversed Sync

Parameters	Value
Server Running	True
Clients Allowed to set time	False
Synchronization Interval (sec.)	20

Table 38. Time Sync Configuration in Clients and Servers: Reversed Sync

		Node Type		
		AC 800M Connectivity Servers	Advant Master Connectivity Servers	Other 800xA System Nodes
CNCP Role		<not used>	<not used>	<not used>
AC400 Time Adaptor		Not installed	Installed	Not installed
Other Time Adaptors		Not installed	Not installed	Not installed
AfwTime Service Role		<not used>	Just executing the AC400 Time Adaptor	<not used>
Time Service Provider Definition	Enabled	False	True	False
TimeServerHandler	Time Synchronization Running	False	False	False
	Allowed to set time	False	False	False
MB 300 Clock Synch Role		<not used>	Master	<not used>
MB 300 Clock Sync Config for the Clock Synch DB element on the RTA board	CLK_MAST	<not used>	1	<not used>
	LOC_TIME	<not used>	0	<not used>
	CLK_SEND	<not used>	1	<not used>
REVERSED_SYNC_MODE in Windows Registry		<not used>	1	<not used>
SNTP Role		Client	Client	Client
W32Time	Startup type	Enabled	Enabled	Enabled

Table 39. Time Sync Configuration in Dedicated Domain Controller: Reversed Sync

SNTP Server addresses		w32tm /config /manualpeerlist:"A.B.C.D A.E.F.G" (the addresses of the external SNTP Servers)
W32Time service	Startup type	Automatic
	Server status	Started
Windows Registry parameters for W32Time	NtpServer	Enabled = 1
	NtpClient	Enabled = 1
	Type	NTP (this is set by w32tm /config /manualpeerlist)

Systems with AC 800M HI with Safe Peer-To-Peer

In an Automation System where AC 800M HI controllers communicate via the Safe Peer-To-Peer MMS protocol the time between two controllers must not differ more than 100 ms.

This means that there are fairly high requirements on the accuracy of the synchronization and setting the time with a big adjustment should be avoided. The following methods are recommended to achieve this¹:

1. Let one AC 800M controller, which is not using Safe Peer-to-Peer MMS, synchronize from an external time source as in [External Time Source](#) on page 150 and at the same time be CNCP master for the AC 800M HI controllers that use Safe Peer-to-Peer MMS, see [Figure 68](#) on page 170.
If the connection to the GPS system is lost the re synchronization of the HI controllers is done with CNCP multicast. It may take slightly different time for different controllers to adjust to the new time, but the time when two HI controllers have different time is much shorter (~5s) with this scheme than if all controllers use SNTP as in [alternative 3](#).
2. Use an AC 800M as time source as described in [Local Time Source](#) on page 146. Avoid setting the time manually while the application process is running.
3. Use redundant external time sources as in [External Time Source](#) on page 150 with the addition to use two SNTP servers. Supervise that the SNTP servers are OK. If both SNTP servers lose the connection to the GPS system for a long time there is a risk for a big adjustment when they regain the connection and it may take different time for different controllers to notice the adjustment.

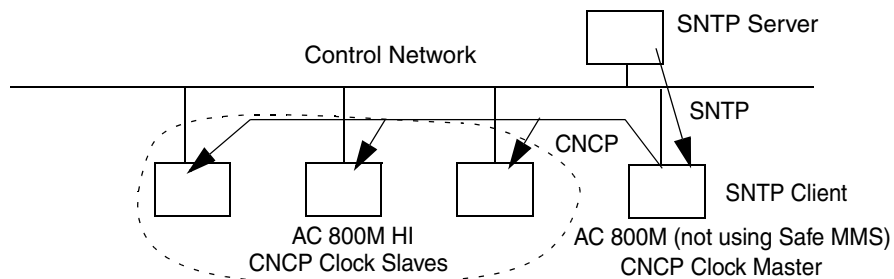


Figure 68. Using CNCP with global time for AC 800M HI controllers

1. The rest of the system can be synchronized with CNCP via the Connectivity Servers as previously described.

Configure Time Synchronization in Controllers

Time Synchronization Parameters for AC 800M

Synchronization of the real time clock in an AC 800M controller is configured in the controller project in the Control Builder. The parameters are located at the bottom of the Hardware editor window for the CPU unit, e.g. PM860/TP860, see [Figure 69](#).

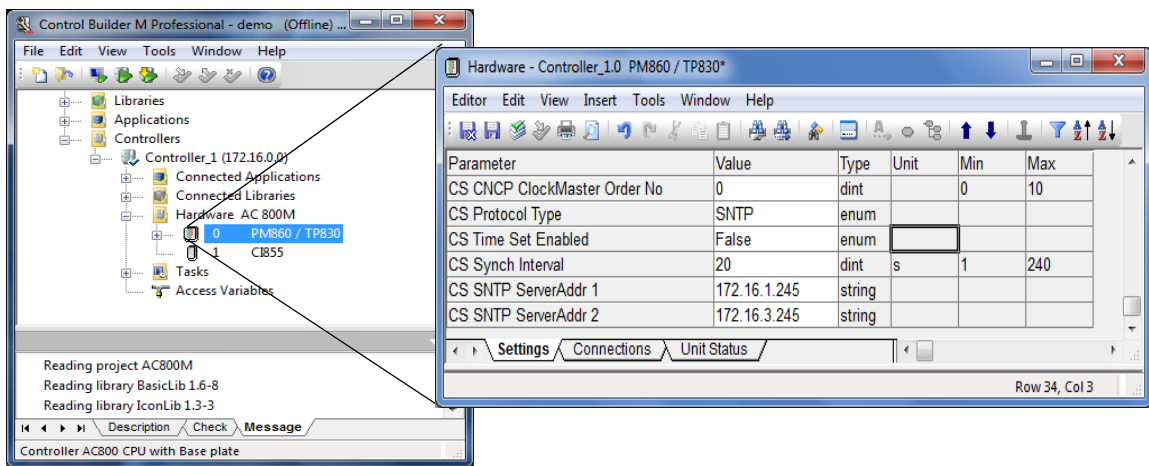


Figure 69. Configuration of Time Synchronization for AC 800M

[Table 40](#) describes the parameters.

Table 40. Parameters Defining Clock Synchronization in AC 800M

Parameter	Type	Value and description
CS CNCP ClockMasterOrderNo	dint	CNCP Clock Master order number: 0: This node can not become Clock Master 1: This is primary Clock Master 2: This is secondary Clock Master n: This is the n' order CNCP Master Max value is 10.
CS Protocol Type	enum	The protocol used for receiving clock synchronization: No Synch: The Controller clock is not synchronized from any other time source. This setting shall be used for a Controller which is root time source for a system. CNCP: The Controller clock is synchronized via CNCP. SNTP: The Controller clock is synchronized via SNTP. MMS: Sync from MMS Date & Time or COMLI is allowed. MB 300: The Controller clock is synchronized from MB 300 via CI855. See Time Synchronization for MB 300 via CI855 on page 173.
CS Time Set Enabled	enum	False: CNCP Time set from network disabled. (recommended if an external time source is used) True: CNCP Time set from network will be accepted. (see Setting the System Time on page 199) “Time Setting” is when the time is changed in a large step, typically manually. Small automatic changes are called “Time Synchronization”.
CS Synch Interval	dint	The clock synchronization interval in seconds: CNCP: The Clock Master transmit interval. SNTP: The interval for poll of Time Server. Default value is 20 seconds. Max value is 240 seconds (4 minutes).
CS SNTP ServerAddr1 CS SNTP ServerAddr2	string	IP-addresses to alternative SNTP Servers If the first entry is zero, no SNTP time requests will be sent.

AC 800M can distribute time via all its supported protocols simultaneously, but it only receives time synchronization via the protocol defined by “CS Protocol Type”. The sending is enabled per protocol:

- The parameter CS CNCP ClockMasterOrderNo controls sending with CNCP. If the parameter is zero the node will not send time with CNCP.
- AC 800M can act as SNTP server. This function is always enabled. The communication initiative lies on the clients so there is no parameter for this.
- The parameter “Time sync” on CI855 controls if CI855 will send time sync on MB 300.

If an AC 800M is root time source for the system (i.e. does not receive time from any other node) “CS Protocol Type” shall be set to “No Sync”.

Time Synchronization for MB 300 via CI855

AC 800M can use the communication module CI855 for time synchronization to or from the MB 300. This is configured with the “Time sync” parameter on the CI855 in the controller project in Control Builder, see [Figure 70](#).

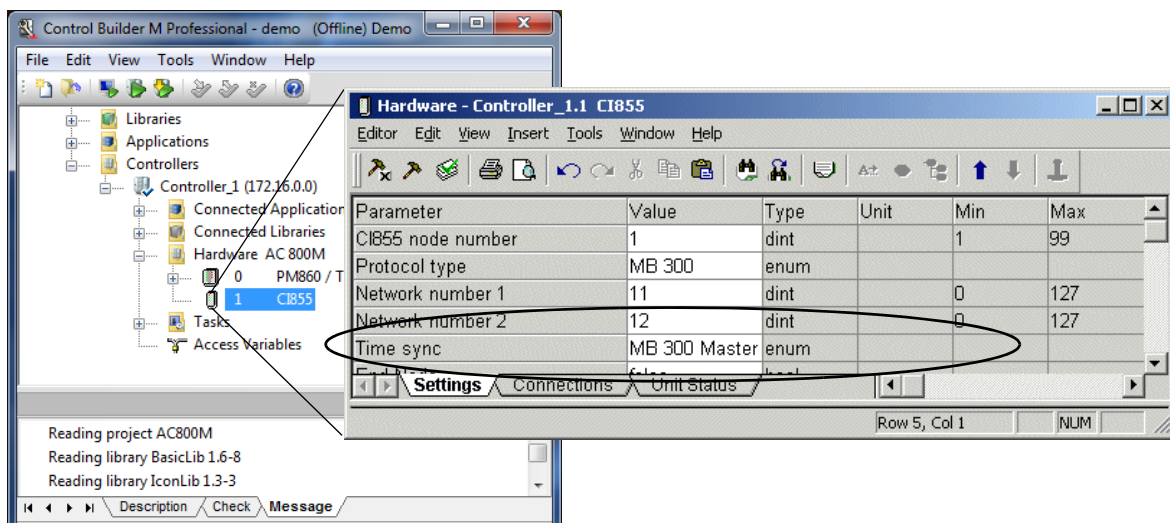


Figure 70. Configuration of MB 300 Time Synchronization via CI855

The Time synchronization parameter on CI855 can be set up according to [Table 41](#) below.

Table 41. Parameters for Defining Time Synchronization of CI855 in AC 800M

Parameter	Type	Value and description
Time sync	Enum	<p>No Time-sync: CI855 is not synchronized.</p> <p>AC 800M Local: CI855 is synchronized from the AC 800M.</p> <p>MB 300 Master: CI855 is synchronized from the AC 800M and acts as a clock sync master on the MB 300 network.</p> <p>MB 300 Slave: CI855 is synchronized from the MB 300 network and synchronizes the AC 800M. (Set also CS Protocol Type = MB 300)</p>



CI855 is the only node type on MB 300 that has both a high accuracy of its local clock, good support for daylight saving time and a possibility to use an external time source. Therefore, it is recommended that the CI855 is set up as “MB 300 Master” on the MB 300 network rather than being used as “MB 300 Slave”.

Time Synchronization in Advant Master Controllers

The time synchronization of an Advant Master controller is configured by the Database Element CLOCK_SYNCH, just like it is done on the RTA board (see [Time Synchronization on the RTA Board](#) on page 190).

CNCP - Control Network Clock Protocol

CNCP is an ABB proprietary master-slave clock synchronization protocol for the Control Network.



CNCP uses RNRP functionality so RNRP must be configured (implicit or explicit) in a node that uses CNCP.

The CNCP Clock Master periodically sends time updates to the clock slaves with multicast messages.

One or several nodes can act as a backup Clock Master. This means that if the current Clock Master is lost, one or several other nodes are prepared to take over as Clock Synchronization Master. To become a backup Clock Master the nodes must be configured for that role. While a node is Clock Master backup it acts as Clock slave and receives time from the active Clock Master.

AC 800M can act as CNCP Clock Master (and as Clock Master backup).

AC 800M and Connectivity Servers with **800xA for AC 800M** with the option AC 800M Time Adaptor installed can act as CNCP Clock Slaves.

Figure 71 shows the node types that can be synchronized with CNCP and their relative time accuracy.

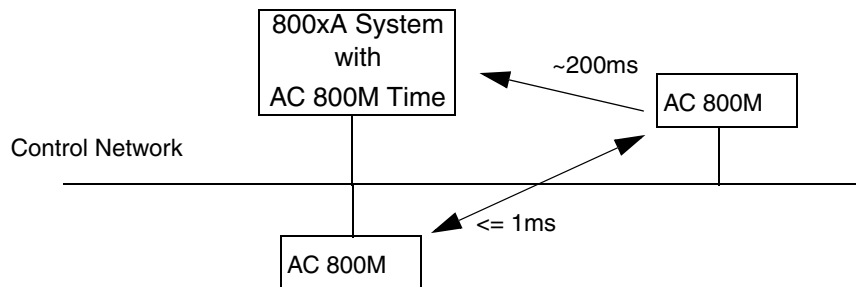


Figure 71. Time Synchronization with CNCP

[Time Synchronization Parameters for AC 800M](#) on page 171 describes how to configure CNCP in a controller. [AC 800M Time Adaptor](#) on page 189 describes how CNCP is used in a PC.



The CNCP messages are received by all CNCP Slaves on the same Network Area as the master independent of which Aspect Directory the nodes belong to. If two 800xA Systems are running on the same network the planning of time Synchronization with CNCP must be done considering both 800xA Systems.



When CNCP is used on a redundant network the messages are sent on both paths. If the backup path is working the messages are taken from this path. The reason is that the amount of traffic is lower on the backup path and this typically gives a better accuracy.

Forwarding of CNCP Between Network Areas

Since CNCP messages uses multicast, the messages are normally not routed between network areas. Standard network routers can be configured to forward multicast but this is not recommended in a system using RNRP and/or CNCP.

An AC 800M controller connected to two different non-redundant network areas can forward CNCP time synchronization between the areas.

SNTP - Simple Network Time Protocol

SNTP is a standard client server oriented time synchronization protocol. It is described in the Internet RFC-2030. The SNTP time clients periodically request time updates from the time server.

SNTP can be used to fetch time from an external time source.

SNTP is a subset of the more advanced NTP (Network Time Protocol) which is described in RFC-1305. The message formats are the same in NTP and SNTP. This means that an SNTP client can use an NTP server.

SNTP Implementations

There are special SNTP implementations that compensate for most known delays (internal and on the network) in the transmission of the time messages from the source to the destination. This can give an accuracy down to +/- 1 microseconds.

The SNTP client implementation in the AC 800M handles some of the known delays. With good SNTP servers, AC 800M can be synchronized with an accuracy better than +/-500 microseconds for nodes connected to the same switch.

The best accuracy is normally achieved with SNTP server usually receives globally synchronized time via a GPS receiver.

The AC 800M controller includes an SNTP server which is always enabled. This server does however not give a very high accuracy.

The Windows Time Service (see [Windows Time Service \(W32Time\)](#) on page 194) in Windows Server 2008 and Windows 7 implements the complete NTP with client and server functionality.

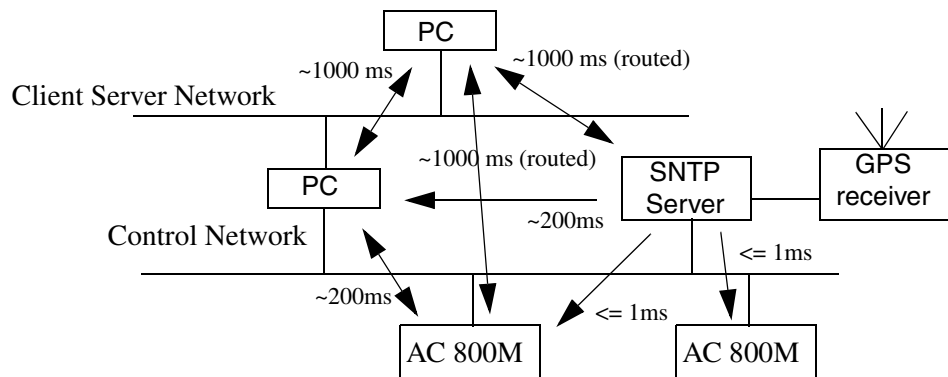


Figure 72. Time Synchronization with SNTP

Stratum

Nodes using SNTP are classified with the term Stratum. Stratum is a value that tells the number of intermediate time servers from an independent global reference time source. An atomic clock is at stratum 0. A time server receiving its time from a stratum 0 source gets stratum 1. An SNTP server with a GPS receiver normally has stratum 1. When AC 800M fetches time with SNTP it informs in the controller log about the stratum of its SNTP server. The stratum of the server does not necessarily say how accurate the clock in the client will be. For example if the transportation delay between the client and the server varies much the accuracy may be bad even if the server has a low stratum and is very accurate. [Fault Tracing Time Synchronization Problems](#) on page 206 describes more about how to check the clock accuracy in different nodes.

SNTP Servers on a Redundant Network

If a redundant network is used the SNTP servers must be duplicated so that there is at least one on each network path i.e. if the SNTP server does not support RNRP.

Routing SNTP Traffic

It is possible to route SNTP communication via an IP router, e.g. a Connectivity Server. This will lead to a lower accuracy than if the Client and the Server are located on the same subnet. This method is recommended for Domain Controllers that do not run the AfwTime Service.

Nodes running RNRP are able to communicate through RNRP routers, as for example the Connectivity Servers, without any special configuration. To enable an SNTP server that does not run RNRP to communicate through an RNRP router the routing capability needs to be configured in the SNTP server. The simplest method is normally to set the parameter for default gateway in the SNTP server to the Control Network address of the Connectivity Server. Note that this must be the address on the network path where the SNTP server is connected, i.e. in the case of an SNTP server connected to the secondary Control Network, it must be the Secondary Control Network address for the Connectivity Server.

Read also about the parameter **Enable TCP/IP Forwarding** in [Table 5, RNRP Configuration Parameters](#) on page 54.

Configuring SNTP

[Time Synchronization Parameters for AC 800M](#) on page 171 describes how to configure SNTP in a controller.

[Windows Time Service \(W32Time\)](#) on page 194, [Enable the SNTP Server, Disable SNTP Client in a PC](#) on page 196 and [Configure Time Synchronization in a Dedicated Domain Controller](#) on page 197 describe how to configure SNTP in a PC.

See also [Fault Tracing SNTP](#) on page 208.

MB 300 Time Synchronization

The time synchronization protocol used on MB 300 is a master slave protocol providing an accuracy better than 3 milliseconds. The protocol is used when time is distributed between 800xA and legacy products in the ABB Master family.

Nodes supporting the MB 300 time protocol are:

- AC 400 Connectivity server via the RTA board PU510 or via the RTA box PU 410.

- AC 800M via CI855
- AC 400 Master, MasterPiece 200, Advant Station 500 OS, MasterGate, etc.

It is recommended to use the CI855 as Clock Master wherever possible. There are two advantages with using the CI855:

- CI855 can distribute time which has been externally synchronized with a high accuracy. This is because CI855 is used in the AC 800M and AC 800M can be synchronized from a high precision SNTP server.
- the CI855 can handle daylight saving shifts.

If CI855 can not be used, it is recommended to use an AC 400 Master controller as Clock Master and to run with a local time source.

In this case the RTA board in the AC 400 connectivity server will act as daylight saving master. This is automatically configured.

An AC 800M using 2 CI855s may forward time synchronization from one MB 300 network to the other. One CI855 is time sync slave on its network, the controller receives the time from that CI855 and the other CI855 is time sync master on its network. This is how you configure the AC 800M if it is used as a replacement of the Master Gate 230/1.

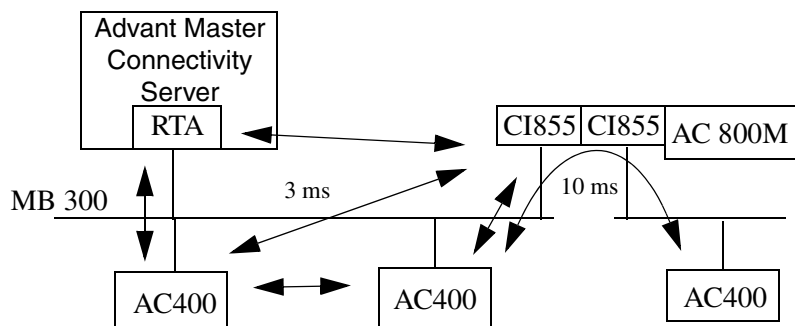


Figure 73. Time Synchronization on MB 300

[Time Synchronization for MB 300 via CI855](#) on page 173,
[Time Synchronization in Advant Master Controllers](#) on page 174,
[Advant Master Time Adaptor](#) on page 189 and [Time Synchronization on the RTA Board](#) on page 190 describe how to configure MB 300 time synchronization.

MMS Time Synchronization

It is possible to set the clock in the AC 800M Controllers and in Panel 800 via MMS. This gives an accuracy between nodes of about 200 ms. The time can be sent from:

- The OPC Server for AC 800M
- Another AC 800M Controller

For Panel 800 MMS is the only supported time sync protocol but the MMS time synchronization should normally not be used for controllers. CNCP and SNTP provide better accuracy.

AfwTime Service

The AfwTime Service can be used to synchronize the time on the server and client nodes defined in a system. This service can also be used to change the current time in the system.

The Time Service has two components, a Time Server and a Time Client.

- **Time Server (Service Provider)**
The Time Server component is the administrator of the time synchronization. It receives and distributes the time synchronization telegrams to/from other nodes, and it makes the final decision on which telegram to accept and broadcast to the network.

The Time Server should be active in the Connectivity Servers. By default the Time Server is installed on all System Product server nodes. There must be at least one Time Server enabled in the network for the Time Service to be operational. If more than one node is configured as a Time Server, only one of the nodes will be active (in Service State), the other nodes will be passive (in Standby State).

- **Time Client (Service Handler)**
A Time Client is responsible for keeping the date and time in its node updated and synchronized with the global time broadcast from the Time Server. It is also responsible for allowing or disallowing manual setting of date and

time, according to how it is configured. A Time Client resides in all 800xA System nodes.

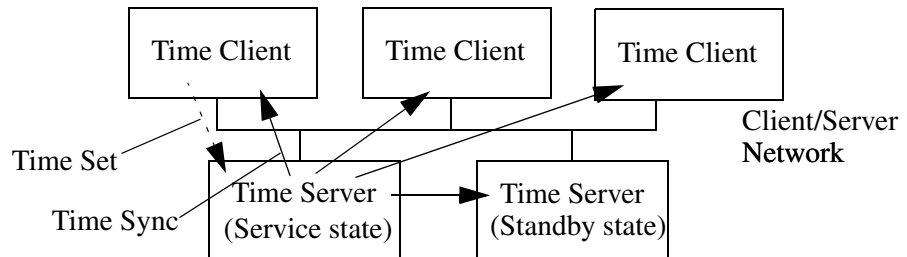


Figure 74. The AfwTime Service

The accuracy achieved is better than 1 second. The operation of the AfwTime Service in a complete system is configured on four types of Aspect Objects:

- The Time Service
- The Time Service Providers
- The Time Server Group
- The Time Service Handlers

The configuration parameters on these different objects are described in the following sections. See also [Fault Tracing AfwTime](#) on page 208.

Configuration of the AfwTime Service

The Service Definition Aspect for the Time Service Object contains Special Configuration parameters that control the operation of all Time Servers (Service Providers) in the system, see [Figure 75](#).

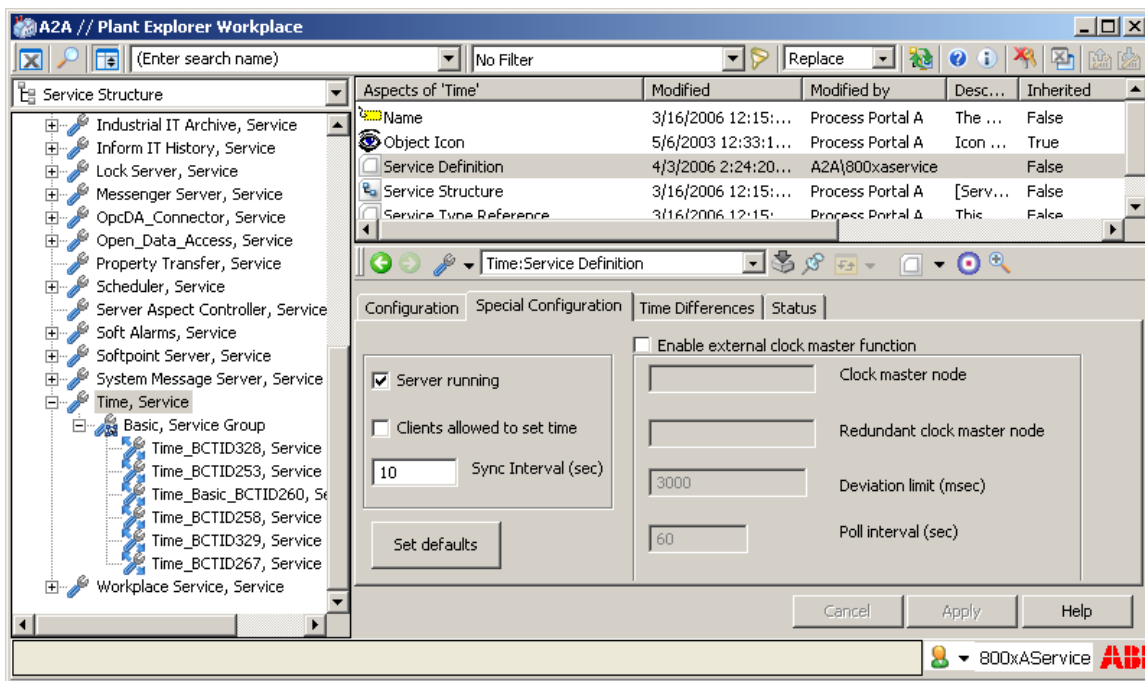


Figure 75. Time Service Definition Configuration Dialog

Table 42 describes the parameters for the Time Service.

Table 42. Parameters for Special Server Configuration

Parameter	Description
Server running	<p>Determines whether the Time Server service must run.</p> <p>If FALSE, no AfwTime server will distribute time and no AfwTime Adaptor will operate.</p> <p>Default value: TRUE</p>
Clients allowed to set time	<p>Determines whether users at client nodes are allowed to set the system time, i.e. the clock on the active Time Server node.</p> <p>Default value: FALSE</p> <p>If this parameter is TRUE and the corresponding parameter on the Time Server Handler aspect on the Node object the Time Server will change its time if the windows time is changed on a client node.</p> <p>If FALSE, the engineer can only change the system time when working on the active Time Server node.</p> <p>This parameter actually decides if the Time Server will accept a time set message sent from a client. The corresponding parameter on the Time Server Handler aspect on the node object prevents the client node from sending the time set message.</p> <p>Set this parameter to FALSE if the system uses an external time source, e.g. a GPS receiver with an SNTP server on the Control Network.</p> <p>Section Setting the System Time on page 199 describes different methods to set the system time. One way is to set this parameter to TRUE and to use windows time to adjust the system time.</p>
Sync Interval (sec.)	<p>This value determines how often synchronization messages are sent to the Time Clients.</p> <p>Default value: 10 sec.</p>

There are additional parameters in the tab **Special Configuration for the Time Service Definition** that can be used if the Time Server must fetch the time from an external time master. This configures usage of an external clock master using *NetRemoteTOD*, which is supported at least by Windows based nodes. This is a synchronization method which is normally not recommended. Receiving the time from a Time Adaptor typically gives better accuracy.



AfwTime’s external clock master function shall not be used if any other Time Adaptor is used.

Configuring the AfwTime Server and the Server Group

The main configuration of the Time Servers is done in the Service Definition. The only item to configure on each Time Server Node is whether the service should run or not, see [Figure 76](#). By default the Time Server is enabled in all Server nodes.

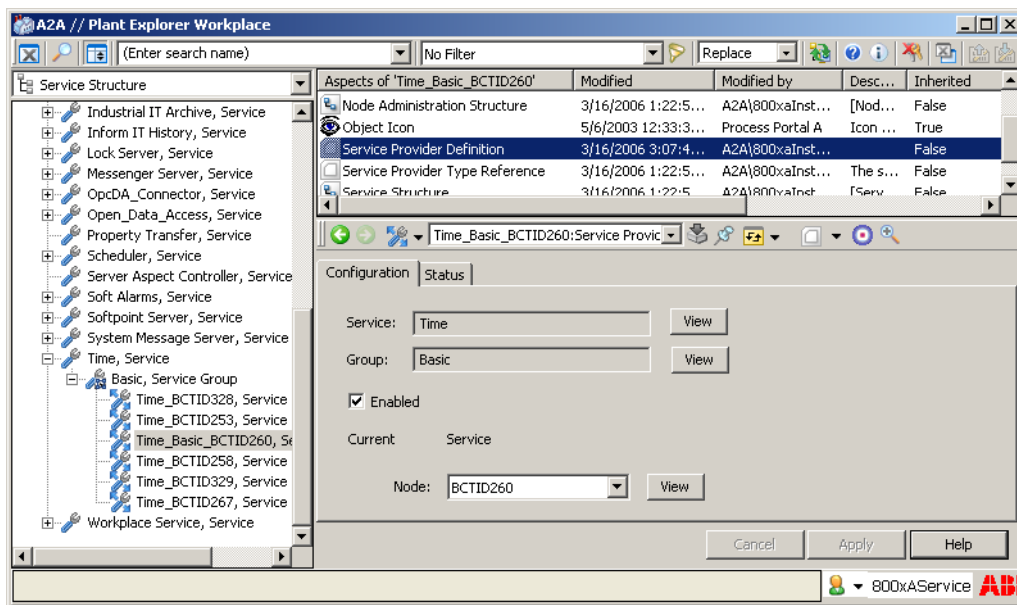


Figure 76. Enabling the AfwTime Server

The Time Server can get the time from a Time Adaptor, see [Time Synchronization for Connectivity Servers, Time Adaptors](#) on page 188. If you want to use a Time Adaptor for receiving or sending time, the Time Server must be enabled. If there is no time adaptor installed, the Time Server will take the time from the local Windows Time.

The operation of the Time Server depends on its state. In Service state the Time Server distributes time to all AfwTime Clients.

When adding a Time Server to the system, the Time Service provider is automatically added to a service group (the Time Server Group) in the service structure.

The order of the servers in the Server Group list decides the priority between the servers. The server at the top of the list will become active and the others will be in a standby state. If the first in the list does not work the next one will take over. The system creates a default order in the list, but the order can be changed manually, see [Figure 77](#).

By default the Time Server is enabled in all Server nodes. Make sure it only runs in the appropriate nodes. If for example a redundant connectivity server pair are the only servers that can receive time from a control network the Time Server for all other nodes should be deleted from the list of Service Providers.

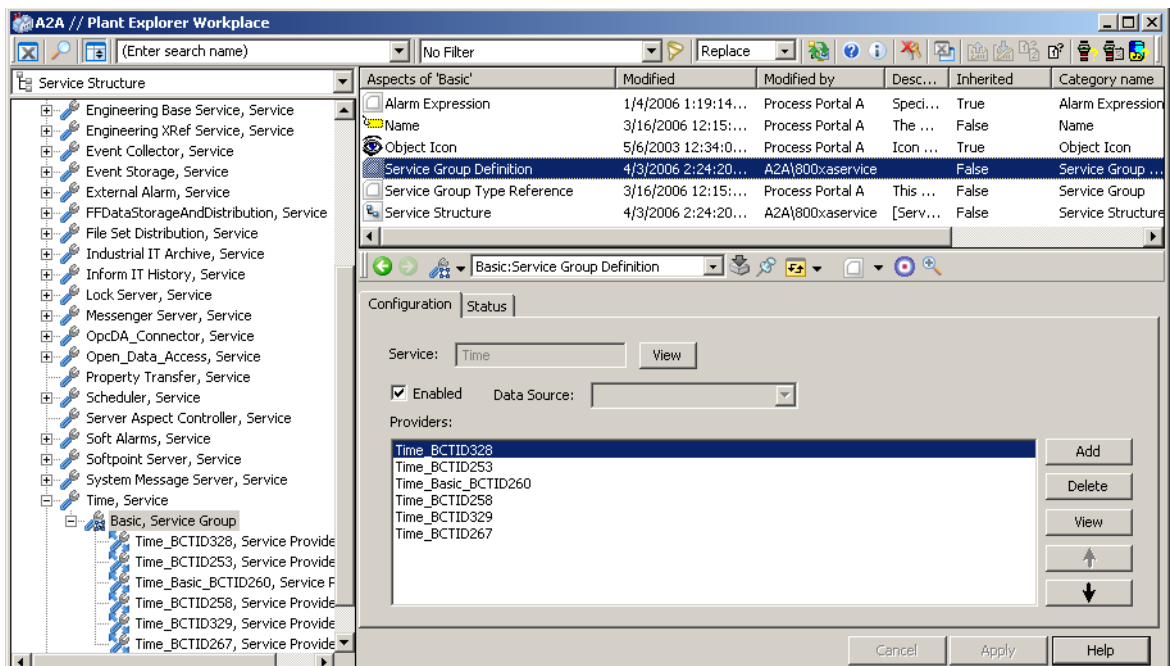


Figure 77. Configuring the priorities for the Time Servers

Configuring an AfwTime Client

The configuration of reception of time synchronization in an 800xA node is done on the TimeServerHandler aspect for the Node object in the Node Administration structure, see [Figure 78](#).

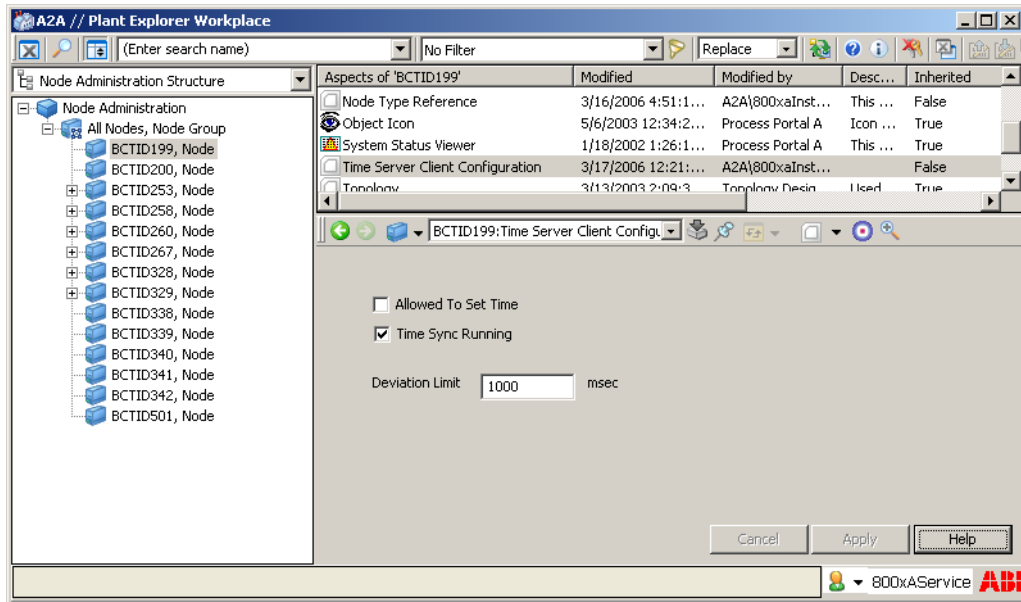


Figure 78. Configuration of the AfwTime Client (Time Server Handler)

Table 43 describes the parameters for the TimeServerHandler.

Table 43. Configuration parameters for the TimeServerHandler

Parameter	Description
Allowed to Set Time	<p>Determines whether a user on this node can set the system time by adjusting the windows time. Section Setting the time for the AfwTime Service on page 203 describes this.</p> <p>Default value: TRUE</p> <p>If the parameter is FALSE, or if the corresponding parameter for the Service Definition is FALSE, a time adjustment in such a node is only executed in the PC where it was done. If that PC is synchronized with some other protocol the change will be over-written the next time the PC is synchronized.</p>
Time Sync Running	<p>Determines whether the node will react when the Server sends time synchronization messages.</p> <p>If FALSE, the Workplace's clock will not be synchronized with the Time Server's clock.</p> <p>Default value: TRUE</p>
Deviation Limit	<p>If the difference between the time in the client node and the time server is less than this value a smooth adjustment is done during a longer time. If the difference is larger the server time is immediately set in the client node in one step.</p> <p>Default value: 1000 msec.</p> <p>The default value may be used.</p> <p>(Value 0 = No synchronization, the Time Sync is disabled.)</p>

Time Synchronization for Connectivity Servers, Time Adaptors

The AfwTime Server receives time synchronization with so called Time Adaptors. There are Time Adaptors for different protocols, for example for CNCP and MB 300. See [AC 800M Time Adaptor](#) on page 189 and [Advant Master Time Adaptor](#) on page 189.



Only one Time Adaptor may be active and synchronizing the AfwTime Server. Since it is not possible to configure which adaptor the Time Server will use, it is recommended to only have one Adaptor installed (or at least only one active) in a PC that will act as AfwTime Server.

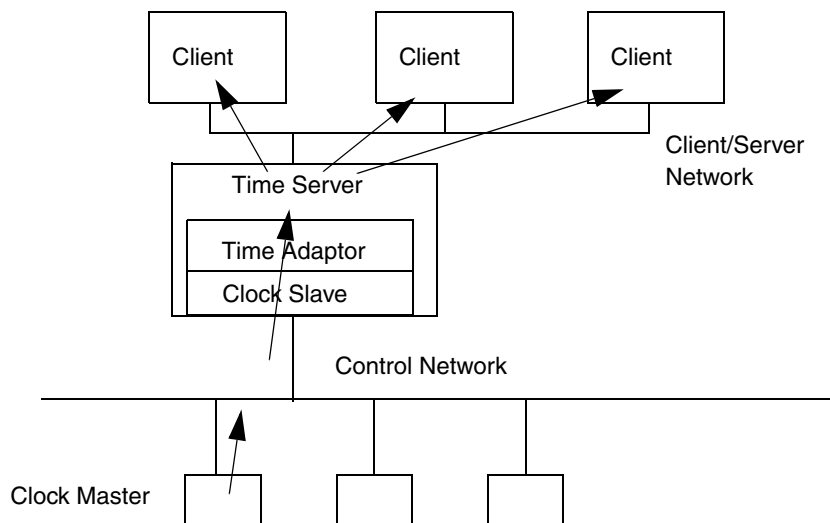


Figure 79. Time Adaptor for the AfwTime Service



A Time Adaptor is only active if the AfwTime Service is enabled and running in Service State in that node

This is a requirement for both receiving and sending of time via a Time Adaptor

AC 800M Time Adaptor

800xA for AC 800M includes the optional AC 800M Time Adaptor that can receive time with CNCP from the Control Network and synchronize the AfwTime Service.

If the time is changed manually in Process Portal, the Adaptor sends a CNCP message to set the new time. This simultaneously sets the new time in all nodes on the control network. See also [Setting the System Time](#) on page 199.

The AC 800M Time Adaptor is installed together with 800xA for AC 800M as follows:

- A typical installation always installs the Time Adaptor
- A custom installation installs the adaptor as optional, default setting is Yes

The AC 800M Time Adaptor is not configurable, so if it is desired not to synchronize the AfwTime Server from CNCP, the Time Adaptor must not be installed in the PC or the Time Server must be disabled.

800xA for AC 800M also includes the OPC server for AC 800M that supports time synchronization via MMS. Disable this feature when CNCP is used.

An AC 800 M Connectivity Server can not synchronize the Control Network from the Client Server network with CNCP. If it is desired to synchronize the nodes on the Control Network from the Client Server network, a node on the Control Network must use SNTP to fetch the time from a Connectivity Server.

This is however, not a recommended synchronization scheme since it typically gives bad accuracy.

Advant Master Time Adaptor

800xA for Advant Master includes a Time Adaptor that can forward time between the RTA board and the AfwTime Service. The default configuration is that the RTA board receives the time from MB 300, the Adaptor reads the time from the RTA board and updates the AfwTime Service.

If the time is changed manually in the Advant Master Connectivity Server and at local time shifts, e.g. daylight saving shift, the Adaptor sends the time to the RTA board which will propagate this to MB 300 to set the new reference time in the system.

To enabling sending time to RTA the TimeServerHandler parameter **Allowed to set time** shall be set to **TRUE**. The default value is **FALSE**, refer [Table 28](#).

Reverse Synchronization Mode

The Advant Master Time Adaptor can be reconfigured to transfer time from the AfwTime Service to the RTA board. This is done from the MB 300 RTA Board object in Control Structure. The instruction *800xA for Advant Master Configuration (3BSE030340*)* describes how to find and modify this parameter. This synchronization direction, however, is not recommended since it gives worse time accuracy to let a PC clock synchronize a controller clock than the other direction. When using reversed synchronization the RTA board should be configured with and CLK_MAST=1, LOC_TIME=0, CLK_SEND=1.

Deactivating Time Synchronization via the Advant Master Time Adaptor

If the Advant Master Time Adaptor should not be used, it can be deactivated by modifying a parameter in the windows registry. This is described in *Industrial^{IT} 800xA, System, 800xA for Advant Master Configuration (3BSE030340*)*. The preferred method is to deactivate the time functionality on the RTA board by setting CLK_SEND=0 and CLK_MAST=0, see [Time Synchronization on the RTA Board](#) on page 190.

Time Synchronization on the RTA Board

The AC 400 Connect uses the RTA board to communicate on MB 300.

The RTA board has the following time synchronization functions:

- Clock Synchronization master on MB 300
- Clock Synchronization slave on MB 300
- Daylight saving time master on MB 300
(This is not configured explicitly)

The time synchronization functionality of the RTA board is controlled by the database element CLOCK_SYNCH. It has the following parameters:

- CLK_MAST
- LOC_TIME
- CLK_SEND

The exact definition of the CLOCK_SYNCH database element can be found in the *Master Net Manual*. The most common combinations are the following:

Table 44. Time Synchronization Configuration for AC 400 Connectivity Server

TIME SOURCE	CLK MAST	LOC TIME	CLK SEND	AfwTime Service	REVERSED SYNC_MODE
AC 800M with CI855 as time source for MB 300, (see Systems with MB 300 and 800xA for AC 800M on page 160) (RTA only receives the time for its own use)	0	2	0	Client on Server off	0
RTA board as time source in the whole system	1	2	1/3	Client on Server on	0
AC 400 as time source in the whole system, RTA as Daylight Saving Time Master (to be used if AC 400 receives external time via minute pulse)	0	2	1	Client on Server on	0
SNTP(W32Time) on the Client Server network (see Synchronization from the Client Server Network on page 167)	1	0	1	Server on	1

The **Afw Time Service** column indicates how the AfwTime Service in the AC 400 Connectivity Server must be used in the different alternatives.



When using an AC 400 Connectivity server as time source for the Client Server Network, the AC 800M Time Adaptor must NOT be installed on that node.

The instruction *800xA for Advant Master Configuration (3BSE030340*)* describes how the Clock Synchronization parameters on the RTA board are modified.

Time Sync with 800xA for Harmony

A Connectivity Server with 800xA for Harmony can receive time from the Harmony Control network and update the local Windows time in the Connectivity Server. A redundant pair of Harmony Connectivity Servers synchronize each other via TSP (=Time Sync Protocol) over the Client Server Network.



The TSP protocol only runs on one network. It does not utilize the RNRP network redundancy on the Client Server network. If the used network path breaks the synchronization stops. Consider this when planning the network connection between the Harmony Connectivity Servers.

To secure the TSP traffic between the Connectivity Servers other ethernet redundancy solutions could be used. The availability of the network path that TSP uses could for example be improved by using ring redundancy or Rapid Spanning Tree, see [Physical Network Installation](#) on page 216.

If a Harmony Connectivity Server is responsible for synchronizing the Client Server network, the AfwTime Server and/or the W32Time SNTP server must be used (see [Configuring the AfwTime Server and the Server Group](#) on page 184 and [Enable the SNTP Server, Disable SNTP Client in a PC](#) on page 196). No Time Adaptors should be installed in the Harmony Connectivity Servers. Configure the AfwTime service as follows:

- Enable the Time Service Providers in the Harmony Connectivity Servers. (See [Configuring the AfwTime Server and the Server Group](#) on page 184)
- Disable the Time Service Providers in all other 800xA nodes.
- Uncheck “Time Sync Running” for the Harmony Connectivity Servers. (See [Configuring an AfwTime Client](#) on page 186)
- Uncheck “Allowed to set time” for all 800xA nodes.

A Harmony Connectivity Server can act as time source for both the Harmony system and the Client Server network.

If a Harmony Connectivity Server is not responsible for synchronizing the Client Server network, it is possible to synchronize it with either the Harmony Control network or with the Client Server network. In the first case the AfwTime Server must be turned off in the node and in the latter case the Connectivity Server must be configured not to synchronize with the Harmony Control network.

For more information about how to configure Time Sync with 800xA for Harmony see *800xA for Harmony Configuration (3BUA000157*)*.

Time Sync with 800xA for Melody

A Connectivity Server running 800xA for Melody can receive time from the Melody O-Net and update the local Windows time in the Connectivity Server. A redundant pair of Melody Connectivity Servers synchronize each other via the TSP (=Time Sync Protocol) protocol via the Client Server Network.



The TSP protocol does not use any network redundancy. The caution note in [Time Sync with 800xA for Harmony](#) on page 192 is valid also for 800xA with Melody.

If a Melody Connectivity Server is responsible for synchronizing the Client Server network, the AfwTime Server and/or the W32Time SNTP server must be used (see [Configuring the AfwTime Server and the Server Group](#) on page 184 and [Enable the SNTP Server, Disable SNTP Client in a PC](#) on page 196). No Time Adaptors should be installed in the Connectivity Servers.

If a Melody Connectivity Server is not responsible for synchronizing the Client Server network, the AfwTime Server must be disabled in the node. The Connectivity Servers itself still needs to be synchronized from the Melody O-Net.

A Melody Connectivity Server only synchronizes from the Melody O-Net to the Client Server network. Not in the other direction. For more information about how to configure Time Sync with 800xA for Melody see *800xA for Melody Configuration (3BDD011741*)*.

Time Sync with 800xA for MOD 300 and 800xA for DCI

The manual *800xA for MOD 300 Configuration (3BUR002417*)* describes how to configure Time Sync with 800xA for MOD 300.

The manual *800xA for DCI Configuration (3BUA000135*)* describes how to configure Time Sync with 800xA for DCI.

Windows Time Service (W32Time)

Windows Server 2008 and Windows 7 supports its own native time synchronization service W32Time. W32Time uses the Network Time Protocol (NTP). The standard configuration for W32Time is that the time is distributed from the Domain Controller to the member nodes in the domain; one of the Domain Controllers act as NTP server and the other nodes act as NTP clients.

Normally W32Time shall be disabled in all nodes that use the AfwTime Service. The exception is when a Connectivity Server is used as NTP server e.g. for the Domain Controller, for an FF HSE Subnet or for some other equipment. Using a PC as an SNTP server is described in [Enable the SNTP Server, Disable SNTP Client in a PC](#) on page 196.

In Windows Server 2008 and Windows 7 W32Time is a complete NTP implementation. It is described in for example in the Microsoft Technet article “Windows Time Service Technical Reference“. It can be found by searching for the article name at <http://technet.microsoft.com>.

Disable/Enable the Windows Time Service

Starting, stopping, enabling and disabling Windows Time Service is done in Windows Services. Set startup type to Disabled if Windows Time is not to be used.

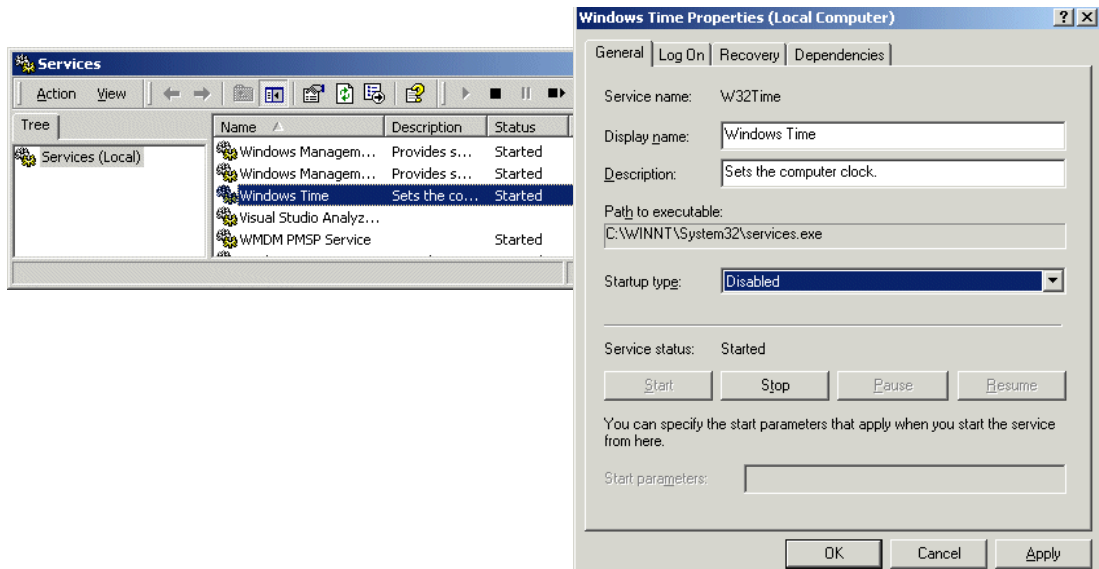


Figure 80. The Windows Time Service in the Services Window

If the goal is to make it possible to synchronize a PC with some other method than Windows Time, an alternative to disabling the Windows Time service is to let it run but to disable the NtpClient function. This is done by setting the value of Enabled = 0 in the Windows Registry system key:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient].

This has the advantage that the NtpServer function can still be used. The NtpServer for example needs to run to make it possible to check time differences between nodes with `w32tm /monitor` or other tools. See more in [Fault Tracing SNTP](#) on page 208.



Windows time must be enabled in FF HSE Connectivity Servers.

Configuring Time Zone and Daylight Saving Time Support

Each PC must be configured for the correct time zone and support for Daylight Saving time for time presentations. This is done with the Windows Date and Time Properties window which can be started from the task bar, see [Figure 81.](#),

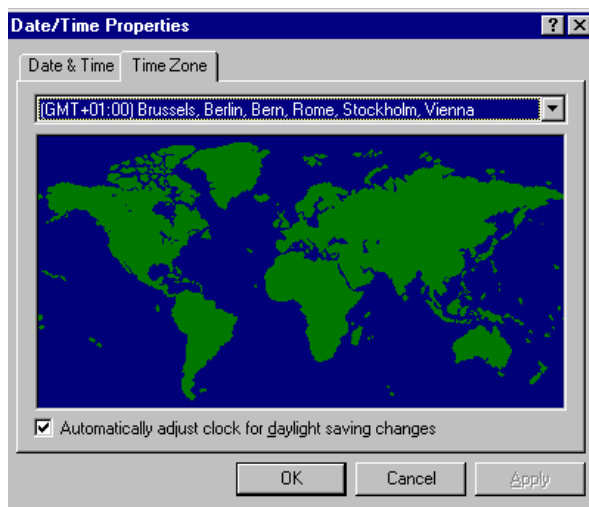


Figure 81. Windows Date and Time Dialog Box

This allows the correct presentation of all times stamps in local time.

All historic data such as Alarms, Events and History data are stored according to UTC time stamps, so their sorting will not be affected, just the presentation will be shown in local time.

Enable the SNTP Server, Disable SNTP Client in a PC

If a PC, which is not a Domain Controller, will be used as an NTP server and this PC is synchronized with other means than w32time (i.e. not with NTP), the following settings must be made on that PC:

1. Open the Windows Registry via the Start menu > Run, type regedit.

2. Go to the System Key:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer]
3. Check that the value of `Enabled` is 1. Set it if it is 0.
4. Go to the neighboring System Key
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient]
5. Set the value of `Enabled` to 0 to disable the NTP client function.
6. Go to the neighboring System Key:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config]
7. Set the value of `AnnounceFlags` to 5 to set the NTP server as “authoritative”.

Independent of which of the above sequences that was used, restart W32Time by the following commands at the command prompt:

```
C:\>net stop w32time  
C:\>net start w32time
```

or restart it from Windows Service Manager,
(see [Disable/Enable the Windows Time Service](#) on page 195).

Configure Time Synchronization in a Dedicated Domain Controller

If the Domain Controller is running in a node that does not run any 800xA software, verify that the clock in the Domain Controller is nearly the same as in the rest of the system. If the time in a node differs more than 5 minutes from the time in the Domain Controller that node will not be accepted by the Domain Controller.

One way of synchronizing a Domain Controller that does not run the AfwTime Service is as follows:

- Install an SNTP server on the same subnet as the Domain Controller or reconfigure the Windows Time Service on one of the nodes that is synchronized from the Control Network system so that it acts as an SNTP server but not as SNTP client (see [Enable the SNTP Server, Disable SNTP Client in a PC](#) on page 196).

- Reconfigure the Windows Time Service in the Domain controller so that it fetches the time from the SNTP server.

To configure a Domain Controller to fetch the time from a specific SNTP server do the following:

1. Start a Windows Command Prompt on the Domain Controller.
2. Stop W32Time and reconfigure it by the following commands:

```
C:\>net stop w32time
C:\>w32tm /config /manualpeerlist: "A.B.C.D"
/syncfromflags:MANUAL
```

A.B.C.D is the IP address of the appointed SNTP server. If more than one SNTP server is to be used in order to get server redundancy, type the addresses separated with blank space(s): "A.B.C.D E.F.G.H".

3. Restart W32Time:

```
C:\>net start w32time
```

4. Request Windows time to re-synchronize once to verify that it works:

```
C:\>w32tm /resync /nowait
```

This should give the printout `This command completed successfully`

Check that there are no error messages from w32Time in the System Log in the Event Viewer in Administrative Tools.

Comparison Between W32Time and the AfwTime Service

This section describes some pros and cons with the Windows Time Service compared to the AfwTime Service for synchronization of 800xA nodes.

The initial configuration effort is typically smaller if W32Time is used

In a standard installation of Windows the default configuration of Windows is that W32Time is used. The default configuration of AfwTime is that the AfwTime Servers are enabled in all servers.

- To use W32Time, disable the AfwTime servers. This is easily done from one node.
- To use AfwTime, disable W32Time in all 800xA nodes. This has to be done on each node. To use the AfwTime service determine which node(s) to use as

Time Server(s). For some cases Time Adaptors needs to be installed. The AfwTime Service objects need to be configured accordingly.

With both methods the Domain Controller anyway needs to be configured to fetch the time from some time source with NTP/SNTP.

It is easier to supervise the operation of AfwTime

- There is no centralized tool to check that W32Time works properly.
- All configuration and operation of AfwTime in all nodes can be done from one (any) 800xA node.

There are tools that can be used for supervision of W32Time, but these are not included in the 800xA System offering.

In a system where time changes need to be easily handled it is recommended to use AfwTime.

Time sync via an Advant Master Connectivity Server needs AfwTime

It is only possible to distribute time via an Advant Master Connectivity Server if the AfwTime Server is running in the node. It is possible to synchronize through the other connectivity server types without using AfwTime.

Tuning the Synchronization Rate for W32Time

It is possible to change the time between time update requests from the a Windows NTP client in Windows Server 2008 and Windows 7. This is done by modifying the windows registry parameter `SpecialPollInterval` which is located in [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient].

To enable usage of `SpecialPollInterval` the parameter `NtpServer` in [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters] needs to be set to a host address followed by the option value 1 written as 0x1, e.g: 172.16.5.245,0x1. (The default value is time.windows.com,0x9).

Setting the System Time

If a controller is used as time source for the entire system (see [Local Time Source](#) on page 146, [Local Time Source](#) on page 146 and [Synchronization from the Client](#)

[Server Network](#) on page 167), it is recommended that all manual time settings are done by one of these methods:

1. If there is a Control Builder M with direct connection to the Control Network, the best method to set the time is via the Time Set function in Control Builder. This sets the time in all controllers on the Control Network simultaneously.
2. Set the time for AFWTime Service on the Connectivity server that is connected to the same Control Network (or MB 300) as the controller that is time source for the system.
This is generally the recommended method for systems with both 800xA for AC 800M and 800xA for Advant Master.
3. Use the function block SetDT in the controller which is clock master.
4. For systems that are synchronized from the Harmony Control Network or the Melody Control Network, the corresponding manuals for the Connect products describe how to set the time.



If an external time source is used, the time should not be set manually. The only exception is during configuration of the system, before the connection to the external time source is working. The time must be reasonably well synchronized in all PCs so that they are not thrown out of the Domain (see [Time Synchronization in a Domain](#) on page 129).



Be careful when changing the system time. Try not to do it when the process is running.

Different functions in the system may behave strangely. Listed below are some examples. There may be others, which are difficult to predict, at least if the time change is large:

- If the time is set backwards the Sequence of Events in Alarm and Event lists may become corrupt. A new event may get an “older” time stamp than an prior events.
You may get similar problems with trend logs. The logs will look strange since there will be two sets of log points for the time that corresponds to the time change.
- If the time is set forward, with a large difference, while the History server is creating logs, the load on the server may increase drastically because it may interpolate log points corresponding to the time jump.
What to regard as a large difference depends on the number of logs and their max time, i.e. the time between interpolated points.
If you for example have 10000 logs with a max time of 10 minutes and make a time change of 100 minutes the History Server needs to create $10000 * 100 / 10 = 100000$ log points. In a normally loaded systems such a burst with more than a couple thousand points may cause problems.
The recommended way to handle a big time change is to disable all active logs first and erase the History files in the directory “Operate IT Data/History”.
- Any substantial time change may cause strange behaviors in active batch processes. What to regard as a big change depends on the timing in the batch process. Stop all active batch processes first if you need to make a big time change.
- If the time is changed in a PC and its Domain Controller at different times there may be problems logging in. Changes of less than 5 minutes are normally OK, see [Time Synchronization in a Domain](#) on page 129.
- If the time is changed in an AC 800M controller Timer function blocks and PID algorithms may give wrong result, since they uses the real time clock.
- If the time is changed at different times in AC 800M HI controllers that communicate via Safe Peer-to-Peer MMS the received data may be marked invalid. This could lead to an undesired process shut down.

The following sections describe how to set the time for the AfwTime Service and how to set the time with Control Builder M.

Setting the Time with CNCP using the Control Builder M

With the Time Set function in the Control Builder M a Set-Time message can be sent with CNCP. The message will be received by all nodes that run CNCP.

The Set-Time message will take effect if the parameter `CS Time Set Enabled` is set to `TRUE`.



Since the Time Set function sends the Set-Time message to all Controllers at the same time this is the recommended method to use in all systems where it is possible.



The Time Set function can only be used to set the time in the AC 800M controllers if the Control Builder is connected to the Control Network with no routers between itself and the controllers to be synchronized. If this is not the case the best method is to use do as in [Setting the time for the AfwTime Service](#) on page 203.

1. Open **Tools > Maintenance > Clock Synch > Time Set**.

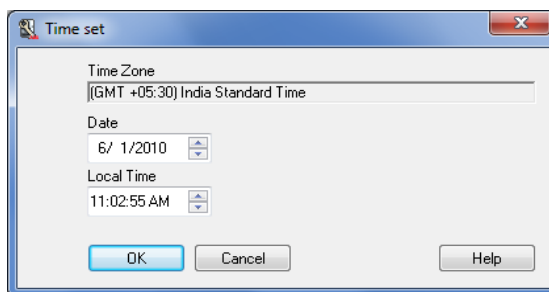


Figure 82. Time Set Dialog in the Control Builder M

2. Enter the new local time to set.
3. Click **OK**.

Setting the time for the AfwTime Service

The time for the AfwTime Service is changed via the normal Windows time function.

The AC 800M Time Adaptors and the AC 400 Time Adaptors in the Connectivity Servers forward the time setting to the Control Network and to MB 300. The AC 800M Time Adaptor does this with the CNCP time set multicast which is also used in [Setting the Time with CNCP using the Control Builder M](#) on page 202.



It is recommended to configure the Windows user rights so that only some users can change the Windows time.



Time changes are done most accurate if they are done as close as possible to the time source network wise. Time changes done via the Windows time function are therefore best done on the connectivity server with the active AfwTime Server.



Do not use this method for changing the time when using 800xA for Melody or 800xA for Harmony. See [Adjusting Time with 800xA for Melody or 800xA for Harmony](#) on page 206.

1. Right-click on the Windows Task bar and select **Adjust Date/Time**.

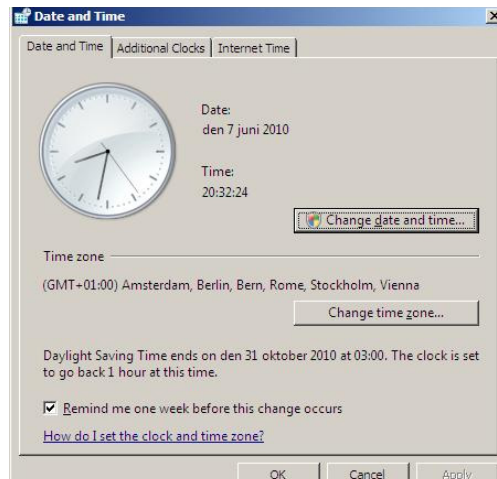


Figure 83. Manually Adjusting the Time from a PC

2. Click Change date and time, Adjust the time and click **OK**.

Adjust the Time in AC 800M via the Function Block SetDT

The function block SetDT has an interaction window that allows the user to adjust the time in the controller with absolute or relative adjustments.

The default template for Controller projects include a Program3 which contains the function block SetTime which is of the type SetDT. The time can be modified with the SetDT function block when an controller application that includes this function block is running in the controller.

To adjust the time with a relative adjustment do the following:

1. Go On-Line to the controller with the Control Builder.
2. Right-Click on the **SetDT** function block in the HW tree or in an on-line editor and select **Interaction Window**.

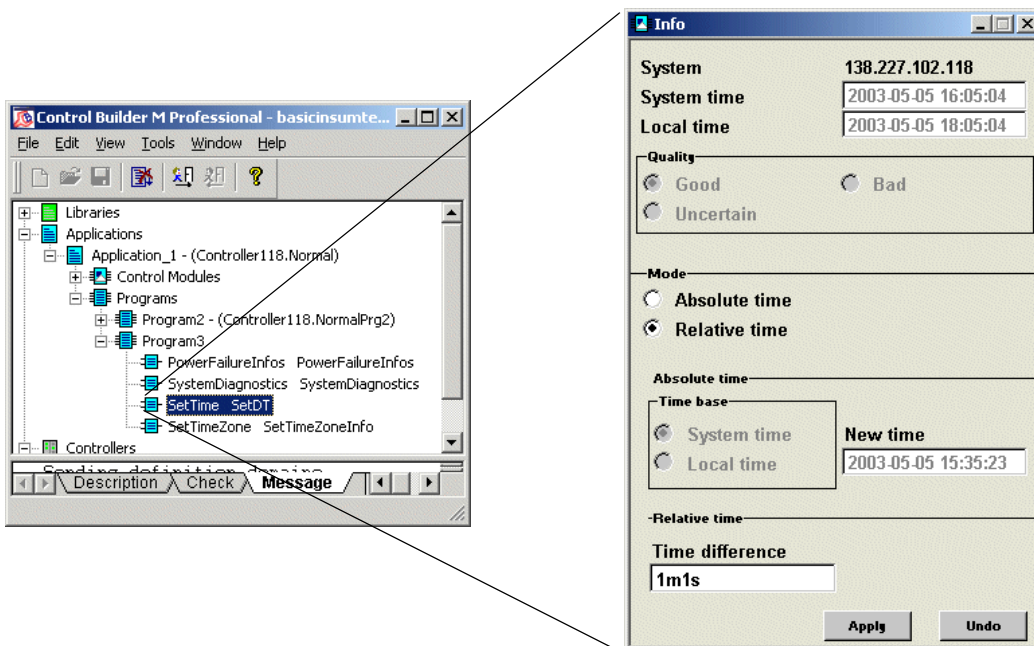


Figure 84. Interaction window for SetDT

3. Mark the check box **Relative time**.

4. Enter the desired clock adjustment in **Time difference**. The time is entered in the format `XdXhXmXsXms` where X represents digits and d, h, m, s, ms represent days, hours, minutes, seconds and milliseconds (see data type *time* in the documentation for Control IT).
Example: Write `1m1s` to adjust the clock 1 minute and 1 second forward.
5. Click **Apply**.

Handling Time Changes when Using W32Time

The standard configuration for the Windows Time Service does not handle time changes well. When a node has joined the domain and has established a working connection with its Domain Controller it only requests time updates every 8 hours. This means that if the time is changed on the Domain Controller it may take up to 8 hours for this change to take effect on all member nodes. Therefore it is recommended to avoid time changes as much as possible when using the standard settings for the Windows Time Service.

If a time change has to be done, it is recommended to trigger a time update on all nodes manually if the time is changed more than 1-2 minutes (see [Time Synchronization in a Domain](#) on page 129). This can be done from a command line with the command line tool **w32tm**.

First make sure that the Domain Controller has received the new time from its source. If it has not, or just to make sure that it does, write:

```
C:\>w32tm /resync
```

This causes the PC to request the time from the SNTP server. The same command may be used on all nodes, but for all nodes except the Domain Controllers it is possible to handle everything from one PC. With the option “-s” the name of another PC can be given. To request “client1” to request new time from the Domain Controller write:

```
C:\>w32tm /resync /computer:client1
```

A successful response that tells that the PC made an attempt to resync is:

```
RPC to server client1 returned 0x0
```

This however does not mean that the resync attempt was successful. This should preferably be checked manually.

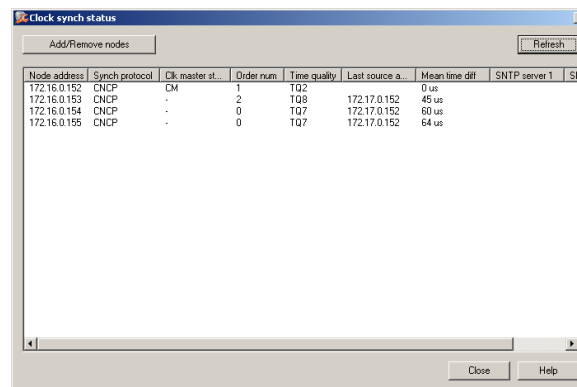
Adjusting Time with 800xA for Melody or 800xA for Harmony

800xA for Melody and 800xA for Harmony include special features for time adjustments and time setting. These features are described in the respective manuals: *800xA for Harmony Configuration (3BUA000157*)* and *800xA for Melody Configuration (3BDD011741*)*.

Fault Tracing Time Synchronization Problems

Fault Tracing Time Sync in Controllers

The Control Builder includes a tool to supervise the clock sync status in controllers. The Clock Sync Status tool can be found under **Tools > Maintenance > Clock Sync > Status**.



Node address	Sync protocol	Ck. master st.	Order num	Time quality	Last source a.	Mean time dif	SNTP server 1	St
172.16.0.152	CNCP	CM	1	TQ2		0 us		
172.16.0.153	CNCP	-	2	TQ8	172.17.0.152	45 us		
172.16.0.154	CNCP	-	0	TQ7	172.17.0.152	60 us		
172.16.0.155	CNCP	-	0	TQ7	172.17.0.152	64 us		

Figure 85. The Clock Sync Status tool in the Control Builder

The Clock Sync Status tool can tell the following about the real time clock in a controller:

- Protocol by which the controller receives its synchronization.
- If the controller currently is CNCP Master or not.
- Configured CNCP Master Order number.
- Time Quality, see [Table 45](#).
- Last time source address.
- Mean time difference the last 60¹ synchronizations.

- Configured SNTP server addresses.

Table 45. Time Quality of the Clock Object in a Controller

TQ	Relative error to the time source
TQ0	Time Quality undefined
TQ1	Time Undefined
TQ2	Not externally synchronized
TQ3	error > 100 milliseconds
TQ4	error < 100 milliseconds
TQ5	error < 10 milliseconds
TQ6	error < 1 milliseconds
TQ7	error < 100 microseconds
TQ8	error < 25 microseconds

The Clock Sync Status tool can only show the status for Controllers.

AC 800M may write clock sync status information in the Controller Log. These are some examples of what this can say:

CNCP:

- Time Set message is received

SNTP:

- Synchronization interval
- The address of the used server
- The Stratum of the server (see [Stratum](#) on page 177)
- If there is no connection to any server
- If the found server (or servers) is not accepted for some reason, e.g. because it is not synchronized.

1. The evaluation of Time Quality uses a shorter filter than the mean time difference. This means that the mean time difference may indicate a better time quality than the TQ value.

MB 300/CI855:

- System messages with Message Type 17 and Code 11. Data 1 may say:
 - 3 = There might be more than one backup time master. Data 2 = Bup Node
 - 4 = More than one Clock Master on the network

Fault Tracing SNTP

SNTP time sync problems can be analyzed with the windows command line utility w32tm.

The Microsoft Knowledge Base Article 816043 describes how to turn on debug logging in the Windows Time Service for Windows Server 2008 and Windows 7.

Fault Tracing AfwTime

The status of the AfwTime service providers can be supervised on the Service Group Definition in the service structure, see [Figure 86](#).

Node	Def. Type	Service	State	Status	M	Process	Start time	Last command	Master Candidate	Configuration	Gr...	Provider	Target
BCTID253	Registered	Time	Undefined	0x0		0	<ZERO TIME>	Undefined	{00000000-0000-0...	Reg:Time/Basic/Time_BCTID253	Basic	Time_BCTID253	Service
BCTID258	Registered	Time	Undefined	0x0		0	<ZERO TIME>	Undefined	{00000000-0000-0...	Reg:Time/Basic/Time_BCTID258	Basic	Time_BCTID258	Service
BCTID260	Registered	Time	Service	0x0	X	768	4/3/2006 10:49:44 AM	Run	Time_Basic_BCTID260	Reg:Time/Basic/Time_Basic_BCTID260	Basic	Time_Basic_BCTID260	Service
BCTID267	Registered	Time	Standby	0x0		2920	4/4/2006 10:10:54 AM	Run	Time_Basic_BCTID260	Reg:Time/Basic/Time_BCTID267	Basic	Time_BCTID267	Service
BCTID328	Registered	Time	Undefined	0x0		0	<ZERO TIME>	Undefined	{00000000-0000-0...	Reg:Time/Basic/Time_BCTID328	Basic	Time_BCTID328	Service
BCTID329	Registered	Time	Undefined	0x0		0	<ZERO TIME>	Undefined	{00000000-0000-0...	Reg:Time/Basic/Time_BCTID329	Basic	Time_BCTID329	Service

Figure 86. AfwTime Service Provider status

State must be “Service” for one service provider and “Standby” for all others. The column “M” (=Master) contains an X for the same node. This is the current time source.

On the Time Service Definition there is a window that shows the time difference between different 800xA nodes, see [Figure 87](#).

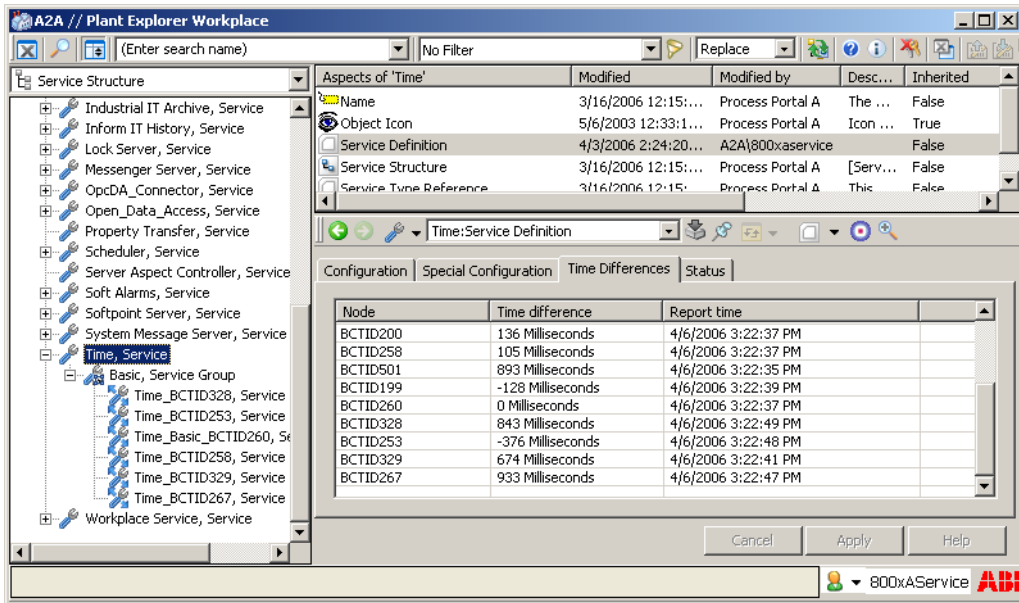


Figure 87. Time Difference Supervision

Section 8 Ethernet and Network Equipment

Ethernet is used for the Control Network, the Client Server Network and MB 300. Some fieldbuses also use Ethernet, see [Section 4, Field Networks](#). This section describes how to plan and build these Ethernet networks and the equipment needed.

Building a Physical Network

Most network diagrams show logical networks only and not physical networks. When you implement them into the real physical networks, you connect systems/nodes to Ethernet hubs or switches. You design each Network Area, in principle, using a star topology. If you want a Network Area to have redundant paths, you must then duplicate all network components (full redundancy).

Below is an example of a Control Network shown first with a logical view, and then with a physical view.

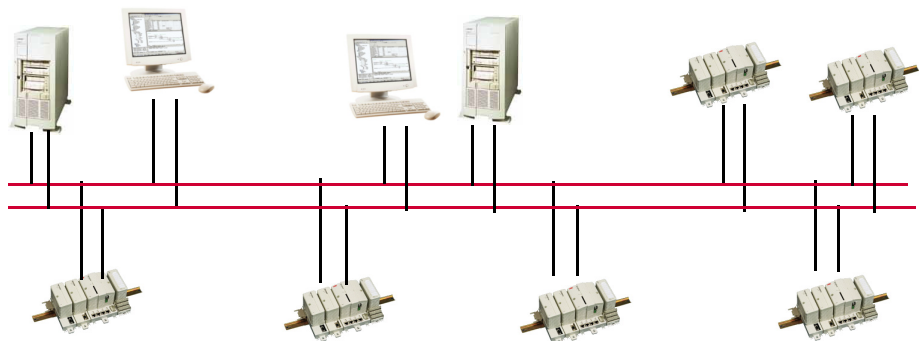


Figure 88. Logical View of a Redundant Control Network

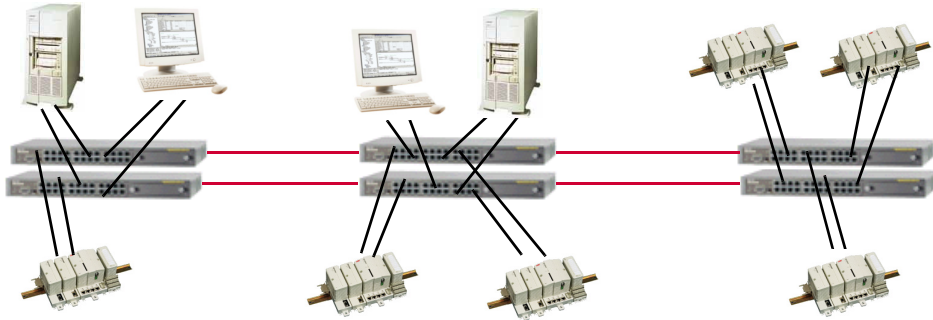


Figure 89. Physical View of the Redundant Control Network

Hubs and Switches

A hub is a connection device within a network segment. It is an Ethernet multiport repeater. A hub only allows one message to be transferred at a time between all of its ports. This means that there will be message collisions when more than one node transmits at the same time, just as it used to be with the old coax cables. Collisions are handled by the media access mechanisms of Ethernet, but in a network with heavy traffic the collisions decrease the data throughput and give non-deterministic response times in the network.

A more sophisticated type of hub is sometimes called a switched hub, but normally just a network switch. A switch is a connection device within a network segment. It filters and forwards frames based on the destination address of each frame. A switch eliminates most of the message collisions caused by several nodes transmitting at the same time. This is basically accomplished by queuing messages per port and by allowing several point-to-point messages to be transferred simultaneously, if they go between different pairs of ports. This means that a network using switches will allow a much higher throughput than a network using hubs and it does not have the same problem with non-deterministic response times.



Even if the basic idea behind switches is conceptually better than that behind hubs, there are differences between different switch products that can have a large influence on the actual network bandwidth. See [Features in Switches](#) on page 213. A poor switch may behave just like a hub under high network load.

In addition, hubs can not be supervised by network management tools.

Features in Switches

A switch is not altogether an ideal device. The store-and-forward delay introduced by a typical switch is about 25 us. If the switch output port is busy with an other 1518 byte packet, then an extra delay of 122 us may occur when the port speed is 100 Mbps, 1.22 ms when the port speed is 10 Mbps. These delays are no problem for normal system applications, but they do affect the accuracy of the network clock synchronization. In this sense, a few large switches in a star topology are better than many switches in a tree structure. The minimum delay is the sum of the store-and-forward delay in every switch passed.

Managed Switches

Switches that only store and forward ethernet packets without being accessible as nodes on the network are called un-managed switches.

Switches that act as a node with an IP address on the network giving access to network management information are called managed switches. The network management information is for example configuration data for the different ports regarding port speed and status information about number of bytes transferred, check sum errors etc. The amount of management information may differ very much between different switch types.

The actual ethernet packet switching function is often the same for managed and un-managed switches. These are some pros and cons for managed and un-managed switches:

- Un-managed switches are typically cheaper.
- Managed switches give the possibility to supervise the network better.
- Managed switches may give possibilities to control the traffic better by e.g. address based traffic filtering.
- In a small network the additional features of a managed switch may be unnecessary.
- In a large network the additional features of a managed switch may be very useful.

The user must decide what features he/she wants to use in the switches. The following sections list some notable features in switches, some are only available in managed switches.

Basic Requirements on Switches

- Ports in compliance with 10Base-T / 100Base-TX / 1000Base-SX supporting both full and half duplex with RJ45 sockets.
- Fiber ports for connections in noisy environments and for long distance connections.
- Backbone connections need ports with 100Mbps or 1000Mbps.
- Link speed should be possible to set by auto-sensing, but manual configuration is recommended, see [Ethernet Speed](#) on page 215.
- Transmission mode, half or full duplex, should be possible to set by auto-negotiation, but manually configuration is recommended, see [Ethernet Speed](#) on page 215.
- Multicast traffic must be allowed.
- Port status should be visible on LEDs.

These features are normally available in both managed and un-managed switches.

Necessary settings in Managed Switches



For correct continuous operation RNRP requires the following settings:

- Multicasting must be enabled.
- Multicast filtering must be disabled.
- Intelligent Multicast must be disabled.
- IGMP Snooping must be disabled.

Features not Required in Switches

Some features in managed switches that are not used:

- Support for Rapid Spanning Tree and/or Spanning Tree is not required in the network redundancy concept with RNRP, but it may be used as described in the section [Using Rapid Spanning Tree](#) on page 222.

Recommended Features in Switches

- Simple Network Management Protocol (SNMP) and RMON are good tools for network diagnostics and traffic monitoring.
- Switches with built-in Web Server are easiest to manage.
- Switches, for which OPC servers allow the user to build applications accessing network management information via OPC; will allow management of the network from the same tools as the management of the remaining system.
- Switches with Broadcast Storm Limitation can reduce the problems caused by a Network Loop. (See [Ring Redundancy](#) on page 220, [Using Rapid Spanning Tree](#) on page 222)
- Quality of Service (QoS) functions like priority tagging (IEEE 802.1p) are not required for the 800xA System network but it is used for PROFINET IO.

Ethernet Speed

Different network equipment supports different communication speed.

It is recommended that all PCs used in an Industrial^{IT} 800xA System support at least 100 Mbps full duplex.

AC 800M controllers with processor modules PM85x and PM86x support 10Mbps half duplex. This shall be configured as fixed setting for all switch ports where an AC 800M is connected, i.e. Auto negotiation shall not be used for these ports. For a managed switch the setting is typically done via the management interface for the switch. There are un-managed switches where the setting can be done with physical switches.

AC 800M controllers with processor modules PM89x support up to 100Mbps full duplex

Nodes with different communication speeds can normally be connected to the same switch and it is normal to connect the Connectivity Server with 100Mbps to the same switch as the controllers that use 10Mbps.

It is however recommended to avoid mixing different speeds in a switch whenever possible, since multicast traffic to the slow devices may also slow down the performance of the nodes using higher speed.

When using 10Mbps and 100Mbps, it is always recommended to manually set the speed and duplex parameters for the ports on both ends of the cable to maximize switch performance and ensure a stable link. Depending on the type of network equipment auto negotiation for 10Mbps and 100Mbps may cause network performance problems. With some combinations of network equipment auto negotiation for 10Mbps and 100Mbps works OK, but it is always a safer choice to configure it manually. In systems where it normally works fine with auto negotiation the performance may still be improved by manually configuring the ports. For 1Gbps, auto negotiation is mandatory and must always be enabled.

Testing network performance

After having installed the network a method to check that it gives the desired performance is to measure how long time it takes to copy a large file (500-600 MB) between the nodes. At 100 mbps full duplex, this transfer should take less than a minute. If it takes more than a minute, the port and NIC settings need to be examined.

Physical Network Installation

The following sections contain recommendations and considerations on how to plan the physical installation.

Ethernet Cables



Use Twisted Pair cables only in areas with common grounding.
Use Optical Fibres in all other cases.

- Normal copper cable installations use RJ-45 connectors and a category 5 or higher Shielded Twisted Pair (STP) cable.

Use CAT5 or higher cables on 10Mbps connections.

Use CAT 5E cables on 100Mbps connections.

Use CAT 5E or 6 on 1000Mbps connections.

- With the STP cable, you can obtain a 100 m maximum distance between the end-nodes in the network segment.
- Separate the cables for the two redundant networks as much as possible, e.g. by using different cable ducts, to limit the risk of simultaneous problems on both networks.
- Use as few types of cables as possible. Avoid using crossed cables.

Allocating nodes to switches

- Nodes that communicate frequently with each other should be connected to the same switch. If this is not possible, keep the number of switches between the communication partners as low as possible.
- In a network with many switches and where all nodes communicate roughly equally with each other, a tree structure of switches is preferable to a chain structure. This is because a tree structure decreases the maximum number of switches between two communication partners.

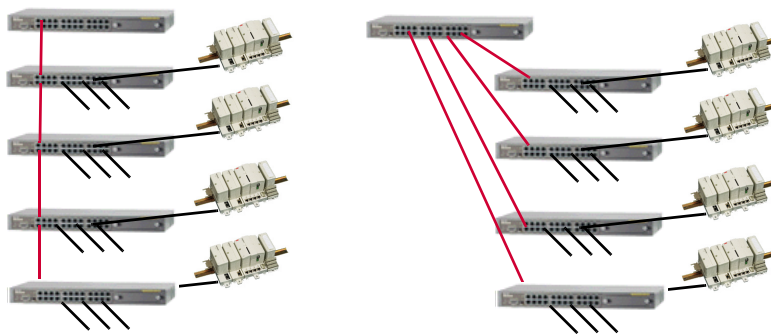


Figure 90. Serial (left) or Tree (right) Network Structure

- Connect nodes with the same communication speed to the same switch (see [Ethernet Speed](#) on page 215.)

Coexistence of Network Types

Ethernet allows several protocols to share the same network. Using the same network for many purposes may reduce installation and maintenance cost.

Combining multiple protocols may, however, lead to unexpected coexistence problems. The basic rule to minimize these is to use separate networks for different protocols.

For many protocols the possibility to share the network or not only depends on the needed network bandwidth for the different protocols, but for some protocol combinations there are special reasons not to share the network.

- Nodes from different security zones should never be connected to the same network, except for the firewalls connecting the zones.
- Most industrial protocols are lacking security functions such as authentication and encryption. To reduce security risks when using unprotected protocols the security zones should be kept as small as possible, i.e. connect only nodes that really communicate with each other to the same network. Nodes with different protocols do not communicate and should therefore be kept isolated.
- Protocols using normal TCP/IP (with unicast, i.e. one-to-one communication) can normally share the same switched network. For these protocols the traffic is properly separated just by making sure that the IP addresses for the nodes on the network are unique. **Modbus TCP** belongs to this protocol category.
- High traffic rates with protocols using multicast or broadcast may cause a high CPU load on nodes connected to the network also for nodes that do not participate in the communication. This is because broadcast and multicast traffic in many cases can not be efficiently filtered by the Ethernet MAC controllers. There are functions in network switches to improve the situation. Consult the vendor of the network component before using these for a specific Field Network protocol. **FOUNDATION Fieldbus HSE, IEC 61850 GOOSE, EtherNet/IP** use multicast. Do not combine any of these protocols with the Control Network.
- Protocols using broadcast or multicast may interfere with each other if they are combined on the same network. For some protocols it depends mainly on the

traffic rate if they can be combined or not but for some protocols also other aspects need to be considered such as for example which MAC addresses that are used. Consult the vendor of the network component before deciding on a specific combination of multicast based protocols.

- Some protocols, e.g. **PROFINET IO**, use Quality of Service functions according to IEEE 802.1p to get higher traffic priority in the switches. This means that other protocols will get less bandwidth.
- VLAN technology (see below) may be used to run different logical networks on the same physical links, e.g. one MB 300 network together with the primary path of the Control Network and another of the MB 300 networks together with the secondary path of the Control Network.
- Most protocols can share the physical network by using VLANs, but several MB 300 networks must still not use on the same physical network since the same set of MAC addresses are used on all MB 300 networks.

Reducing HW using Virtual LANs

Installing a network using several separate networks can in some cases be simplified by use of Virtual LANs; VLANs. Most managed switches support VLANs. When using VLANs the ethernet ports in the switches are configured to belong to one (or more¹) VLANs or to run VLAN tagged traffic (aka trunk ports). The ports with tagged traffic transport packets belonging to all VLANs. Each packet is tagged with information about which VLAN it belongs to. The untagged ports transport only packets belonging to a certain VLAN. This makes it possible to build a network where several networks share the physical media between switches but the nodes connected to untagged ports for different VLANs do not receive traffic from each other. The right hand part of the system configuration described in [Figure 26](#) on [page 77](#) can be implemented as shown in [Figure 91](#).

1. All switches may not be able to configure untagged ports belonging to more than one VLAN.

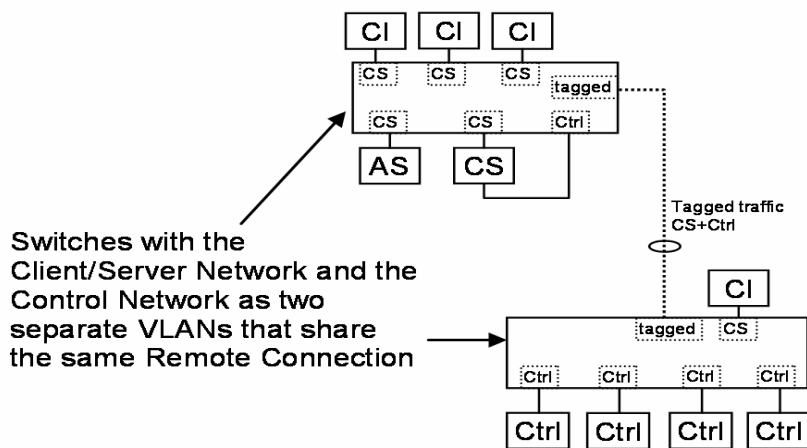


Figure 91. Client/Server and Control network sharing a physical link using VLANs

Usage of VLANs can simplify physical installation because it may reduce the amount of cables and switches but it may make the maintenance more complicated. If a switch needs to be replaced the amount of configuration to do before the new switch can be used increases if VLANs are used compared to if all logical networks are built with physically separate switches.

VLANs can not be regarded as a security mechanism. Do not use VLANs to separate traffic from different security zones.

Ring Redundancy

Some switch vendors support a ring redundancy concept, e.g. the MRP protocol. This normally gives an improved system availability as it provides cable redundancy. The switches themselves are still, however, single points of failure.

You have to consider what type of problems threaten the availability of the network; is it more likely that a fiber optic cable will be destroyed or that a switch will fail.

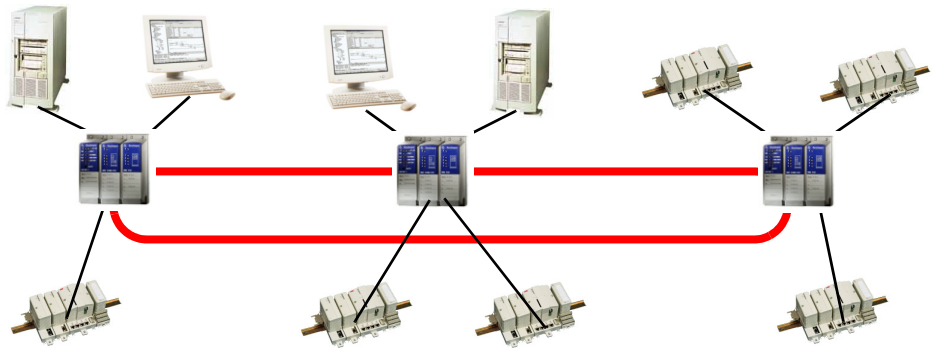


Figure 92. Switches with Ring Redundancy



A misconfigured network with a ring topology may lead to a **network loop**.

A network loop may cause a broadcast storm where the nodes in the network receive the same packets over and over again. A broadcast storm may lead to a load of the network close to its maximum capacity. Most types of host nodes on a network with a broadcast storm experience severe problems, e.g. a Windows based PC is likely to lose network connections, **controllers may shut down**.

When using ring redundancy it is very important to avoid completing the ring physically before the ring redundancy protocol is properly configured. You must also be careful if you plan to change the configuration in a switch which is responsible for the redundancy management. If the redundancy configuration is lost there may be a network loop.

See also [RNR Network Loop Detection and Protection](#) on page 72



We do **not** recommend running the **two RNRP network paths** on the **same physical ring** even if it would be possible to connect the two network interfaces of a node to two different switches.

If redundant switches are required, the two network paths should be physically separated as described in [Figure 89](#) on [page 212](#) because running both paths on one ring:

- gives less protection for “active” Ethernet problems, like for example a continuous sender.
- does typically not save any hardware since the same amount of switches are needed as if the paths are physically separated.

With separated network paths the availability of each path can of course be additionally improved by using one redundancy ring for each path as in [Figure 93](#).

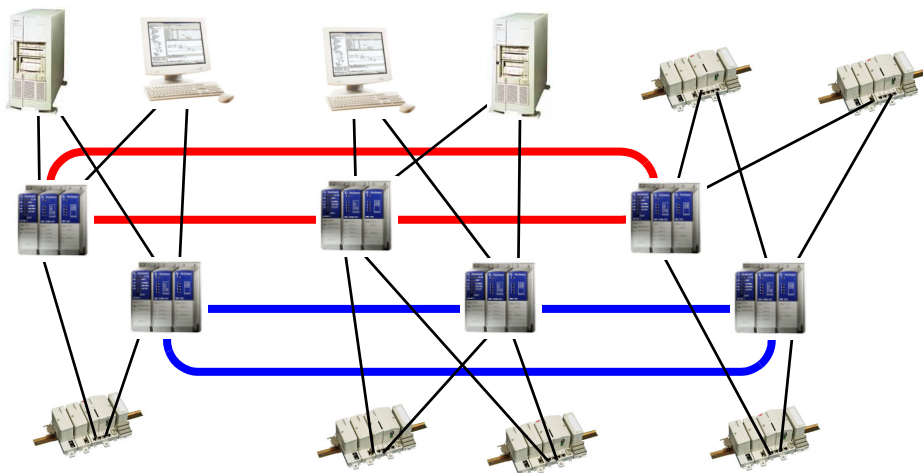


Figure 93. Using Fiber Optic Ring Redundancy and RNRP

Using Rapid Spanning Tree

The Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) provides a mechanism to achieve a network where several switches can cooperate to create redundant communication paths for the nodes connected to the network.

It selects one path and switches to another if the currently used path breaks. In a network with many switches Rapid Spanning Tree is able to create several redundant paths.

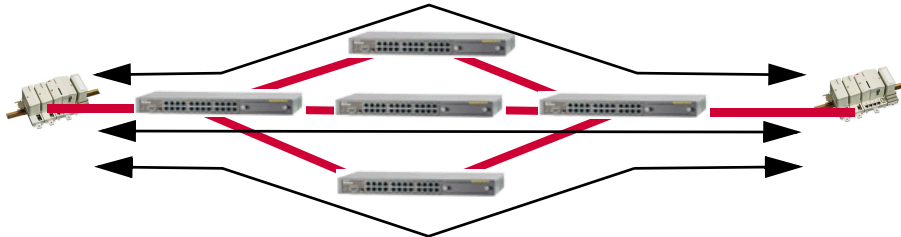


Figure 94. Rapid Spanning Tree manages Redundant Paths in the Network

Like in the case of the ring redundancy Rapid Spanning Tree is a good method to improve the availability in a network with nodes that are connected with single interfaces.

It is possible to combine Rapid Spanning Tree and RNRP redundancy, but as in the standard case in [Figure 89](#) on [page 212](#) and in case of ring redundancy in [Figure 93](#) on [page 222](#) the two paths should be kept physically separate.



A misconfigured network with a multiple paths may lead to a **network loop**.

A network loop may cause a broadcast storm where the nodes in the network receive the same packets over and over again. A broadcast storm may lead to a load of the network close to its maximum capacity. Most types of host nodes on a network with a broadcast storm experience severe problems, e.g. a Windows based PC is likely to lose network connections, **controllers may shut down**.

When using rapid spanning tree it is very important to avoid connecting redundant paths before the rapid spanning tree protocol is properly configured. You must also be careful if you plan to change the configuration in a switch running rapid spanning tree. If the redundancy configuration is lost there may be a network loop.

When Rapid Spanning Tree is correctly configured it actually provides a protection against network loops.

See also [RNRP Network Loop Detection and Protection](#) on page 72



As for ring redundancy we do not recommend connecting the two interfaces of each RNRP node to **two switches** that are on **the same Rapid Spanning Tree network**. Doing this may lead to a network where both RNRP paths are using the same Rapid Spanning Tree path. A break on that path will stop both RNRP paths. The time it will take to heal such a network break depends on the speed of the Rapid Spanning Tree network and this depends on the size of the network. The RNRP switch over time is constant.

When building a redundant RNRP network the availability of each path may, as in the case of ring redundancy, be improved with one separate Rapid Spanning Tree network for each path as in [Figure 95](#).

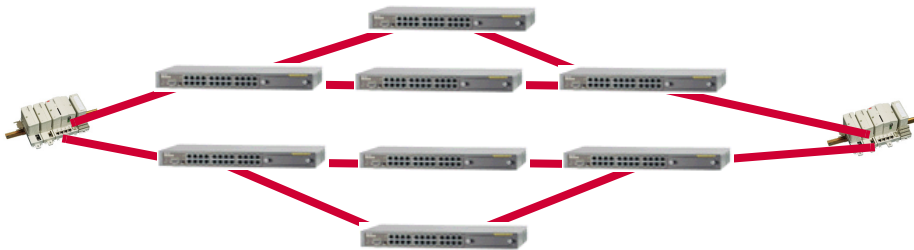


Figure 95. Using Rapid Spanning Tree together with RNRP

Environmental Consideration

The type of network components that you may use depend on the climatic and electrical environment.

In a Non-industrial Application

In an office environment, you can use most world-wide known brand products. It is recommended to use the STP cable.

In an Industrial Application

You have to select products that fulfill industrial requirements on:

- Temperature
- Humidity
- MTBF

- EMC
- Supervision

In the industrial application it is recommended to use the multi-mode fiber 62.5/125 or better 50/125 fiber, 100Base-FX or 1000Base-SX between switches. The maximum distance depends on the speed, fibre type and the network equipment. Special network components can be used to obtain extra long distance.



It is safe to use twisted pair cable only where you have full control of the cabling inside an area with the same common ground, for example inside cabinets or between cabinets in a control room with cabinets connected to a common ground.

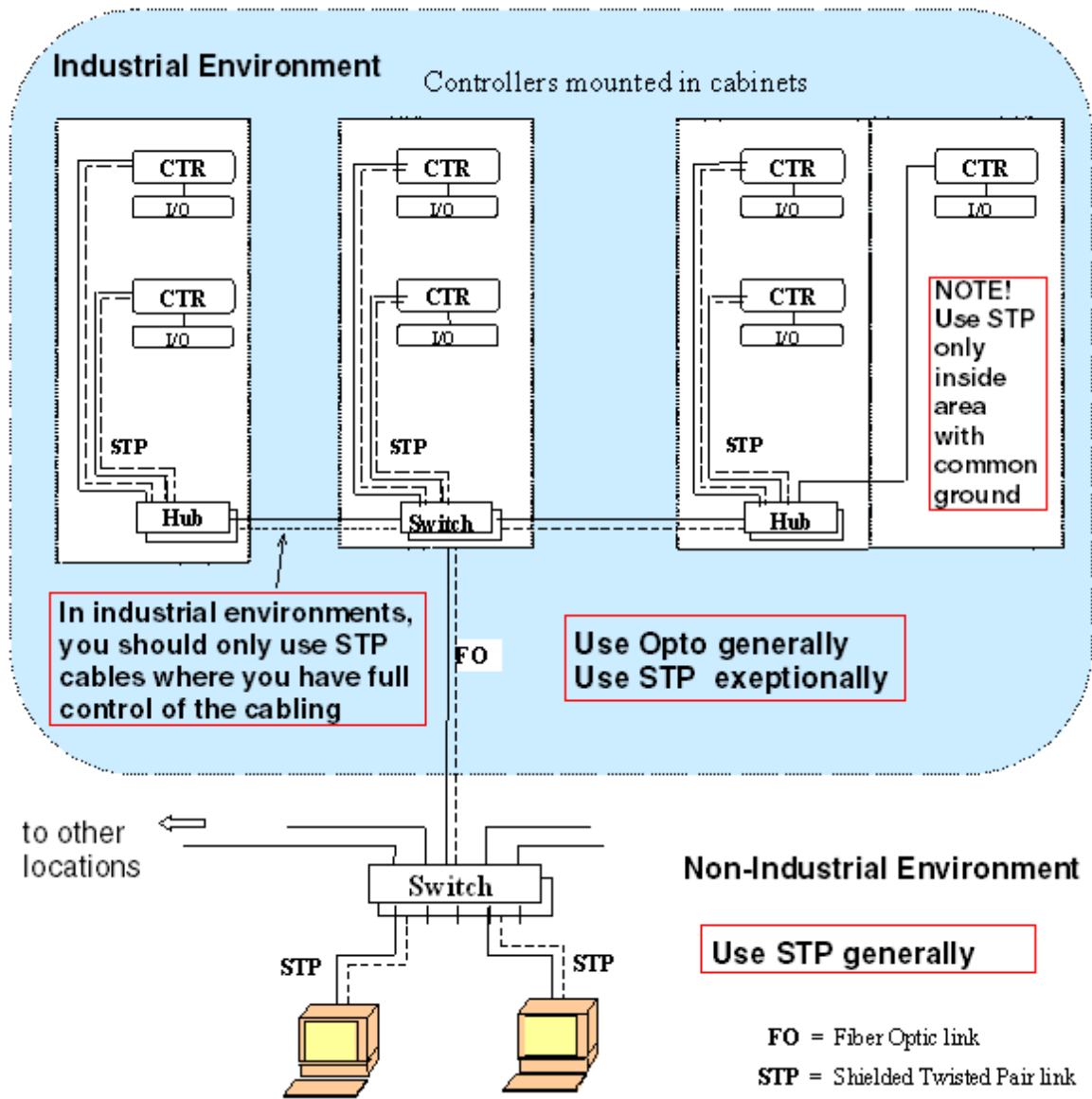


Figure 96. EMC Considerations for a Network Installation

Connecting to a Redundant Network

When nodes are connected to a redundant network it is important that the network interface for the primary network is actually connected to the primary network and vice versa. This is true for both PCs and Controllers. It is recommended to use different cable colors for the two network paths. [Table 46](#) shows one example.

Table 46. Example of Cable Colors

Network type	Color
Client/server Network Primary Path (also for combined Client Server and Control Network)	Yellow
Client/server Network Secondary Path (also for combined Client Server and Control Network)	Orange
Control Network Primary Path	Red
Control Network Secondary Path	Blue
Ethernet based Fieldbus Primary Path	Black
Ethernet based Fieldbus Secondary Path	White

Connecting a PC

When connecting the network to the PC it may be difficult to know which of the two network interface boards is the primary. One way to find out is to do the following:

1. Connect one of the network interfaces cables to the switch.
2. Open the **Network and Sharing Center > Manage Network Connections**.
3. The icons show which of the network interfaces you have connected.
4. Disconnect the network cable.
5. Verify that both network interfaces now are marked disconnected.

Connecting a Controller without CPU Redundancy

When connecting a controller without CPU redundancy simply connect the primary network to the connector CN1 and the secondary network to CN2.

Connecting a Controller with CPU Redundancy

When using the AC 800M with redundant CPUs, e.g. PM861, PM864 or PM865, it is recommended to always also use network redundancy, i.e. using both network interfaces on both Controller CPUs. This means that each AC 800M controller in total has 4 connections to the network. It is important that the primary network interfaces on both CPUs are connected to the primary network.

The best tolerance to network faults is achieved if all the 4 network ports are connected to different switches. Use 4 switches for each group of controllers in the plant as in [Figure 97](#):

- One for the Primary network for all “Upper” CPUs
- One for the Secondary network for all “Upper” CPUs
- One for the Primary network for all “Lower” CPUs
- One for the Secondary network for all “Lower” CPUs

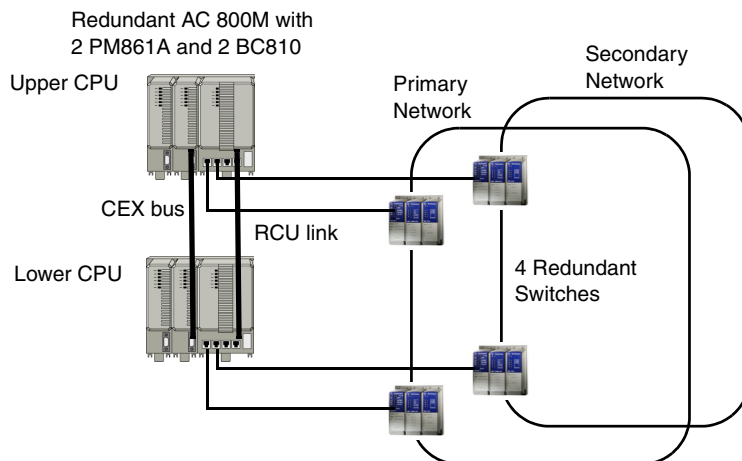


Figure 97. How to Connect a Redundant AC 800M to a Redundant Control Network

If the two network paths are implemented as rings or with some similar kind of ethernet redundancy the complete solution will be very fault tolerant.

Routers

Separate standard non-RNRP routers are normally not used within the Control Network. The routing required between Client/Server Network and Control Network Areas is taken care of by the Connectivity Servers running RNRP. Standard routers may be used for connections between a network running RNRP and an external network. This must in many cases be done with a device which acts as a firewall, see [Interconnecting RNRP Network Areas via Standard IP Routers](#) on page 62 and [Connecting a single Firewall to a Redundant Network](#) on page 104.

Section 9 Network Monitoring and Maintenance

Supervision and fault tracing in the networks can be done in many different ways depending on what is required. The following sections describe some tools and methods for:

- Supervising general network health.
- Checking that one node has contact with another node.
- Checking the network connections in a node.

System Status Viewer

The System Status Viewer is the main Aspect system for on line supervision of the 800xA System. Servers and Controllers have system status providers that show their status. Clients do not have any System Status providers. Connectivity packets may also provide System Status Providers if they handle nodes on a network. Not all connectivity packets include System Status Providers.

The System Status viewer can be added as an aspect on any object. It is by default added at 3 Aspect Objects:

- The node group “All nodes” in the Node Administration structure, see [Figure 98](#). Here all servers and controllers are available.
- The root object “Services” in the Service Structure. Here the status of all AfwServices is available.
- The Root Domain object in the Control Structure. Here the status can be seen for all Controllers and subordinate objects for which their Connectivity packet implements system status providers.

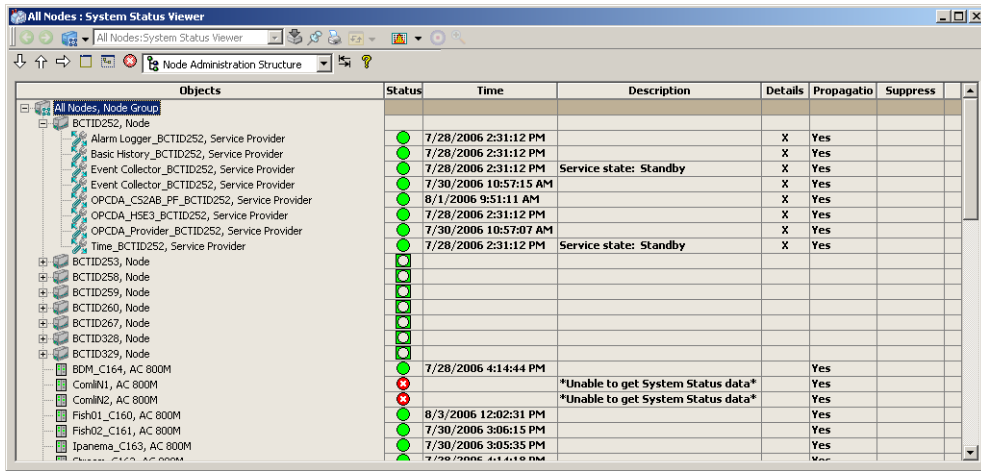


Figure 98. The System Status Viewer with status for Servers and Controllers

AC800M controllers are represented by one object in the node administration structure. In the control structure also the subordinate objects are visible, see [Figure 99](#). By adding a System Status Viewer aspect for the Object representing a Control Network it is possible to show the System Status for all the objects in the Controllers on that Control Network.

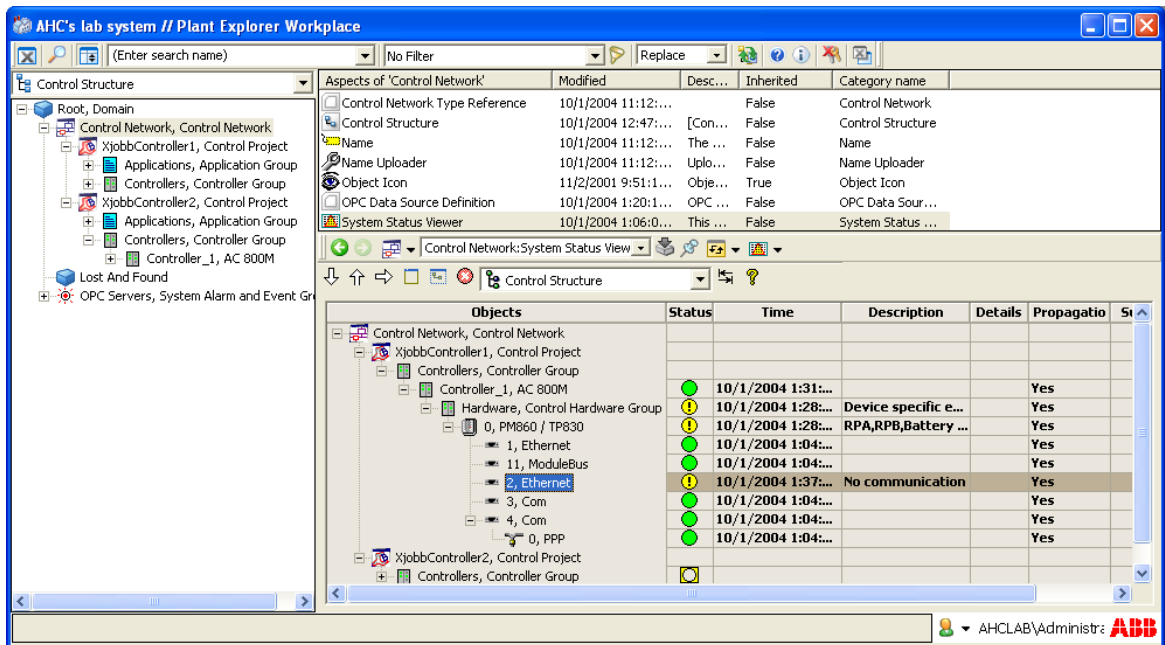


Figure 99. The System Status Viewer with status for Controller Objects

The System Status viewer can show if a controller loses all communication on an ethernet port. This is indicated as **No Communication** as in Figure 99.

Independent of which client is running the System Status viewer it shows the status of all nodes as seen from the aspect servers. In a normal network this is sufficient since all nodes normally see the same other nodes, but for fault tracing special problems where it is interesting to check the connection between two particular nodes the RNRP monitor can be used, see [RNRP Network Monitor](#) on page 237. A particular nodes connections to different servers can be checked with the Afw Service Connection Viewer, see [Afw Service Connection Status Viewer](#) on page 234.

Afw Service Connection Status Viewer

The Afw Service Connection Status Viewer shows the status of services that are used in the node where it is running, see [Figure 100](#).

Status	Service	Group	Provider	Node	Ignored	Areas: 2
●	EventCollector	BCTID260_AC800M_SG	BCTID260	BCTID260	False	⚡⚡
●	EventCollector	BCTID199_AC800M_SG	BCTID199	BCTID199	False	⚡⚡
●	EventCollector	BCTID258_BatchEventSG	BCTID258_BatchEventService	BCTID258	False	⚡⚡
●	Scheduler	IM_BCTID267	IM_Scheduler_BCTID267	BCTID267	False	⚡⚡
●	System Message	Basic	System Message_Basic_BCTID260	BCTID260	False	⚡⚡
●	BackupService	Basic	BackupService_Basic_BCTID260	BCTID260	False	⚡⚡
●	Engineering Base Service	Basic	Engineering Base Service_Basic_BCTID260	BCTID260	False	⚡⚡
●	External Alarm	Basic	External Alarm_Basic_BCTID260	BCTID260	False	⚡⚡
●	External Alarm	Basic	External Alarm_BCTID267	BCTID267	False	⚡⚡
●	External Alarm	Basic	External Alarm_BCTID258	BCTID258	False	⚡⚡
●	External Alarm	Basic	External Alarm_BCTID199	BCTID199	False	⚡⚡
⊗	External Alarm	Basic	External Alarm_BCTID200	BCTID200	False	⚡⚡
●	External Alarm	Basic	External Alarm_BCTID270	BCTID270	False	⚡⚡
●	AssetMonitoring	AssetMonitoring SG_1	AssetMonitoring SP_1	BCTID270	False	⚡⚡
●	OpcDA_Connector	SG_A2_MediumNet_Types_PH	OPCDA_Provider_BCTID260	BCTID260	False	⚡⚡
●	OpcDA_Connector	SG_A2_Type2_6_7	OPCDA_Provider_BCTID260	BCTID260	False	⚡⚡
●	OpcDA_Connector	HSE Subnet-HSESubnet2	HSE Service Provider-HSESubnet2	BCTID260	False	⚡⚡
●	OpcDA_Connector	SG_A2_MediumNet_Types_Batches	OPCDA_Provider_BCTID199	BCTID199	False	⚡⚡
⊗	OpcDA_Connector	SG_A2_MediumNet_Types_Batches	OPCDA_Provider_BCTID200	BCTID200	False	⚡⚡
⊗	OpcDA_Connector	HSE Subnet-HSESubnet1	HSE Service Provider-HSESubnet1	BCTID200	False	⚡⚡

Figure 100. The Afw Service Connection Status Viewer

If node A is using a service in node B the Afw Service Connection Status viewer in node A shows the status for the service in node B. If the network is redundant the status of the network paths between node A and node B is also shown. A green flash indicates that the path is working and a red flash indicates that the path is broken.

Figure 100 shows how it looks when the node running the Afw Service Connection Status viewer is using has lost the secondary network path to node BCTID199. It also shows that there is no working connection to the services in BCTID200. Either both network paths are broken or the services are not running in BCTID200.

The Afw Service Connection Status viewer is started with a right click on the green 800xA System icon in the System Tray.

Topology Designer / Topology Status Viewer

With the Topology Designer you can configure graphical network diagrams.

When the network diagram is configured the Topology Designer can also be used as a Topology Status Viewer to show live status information about the nodes in the diagram.

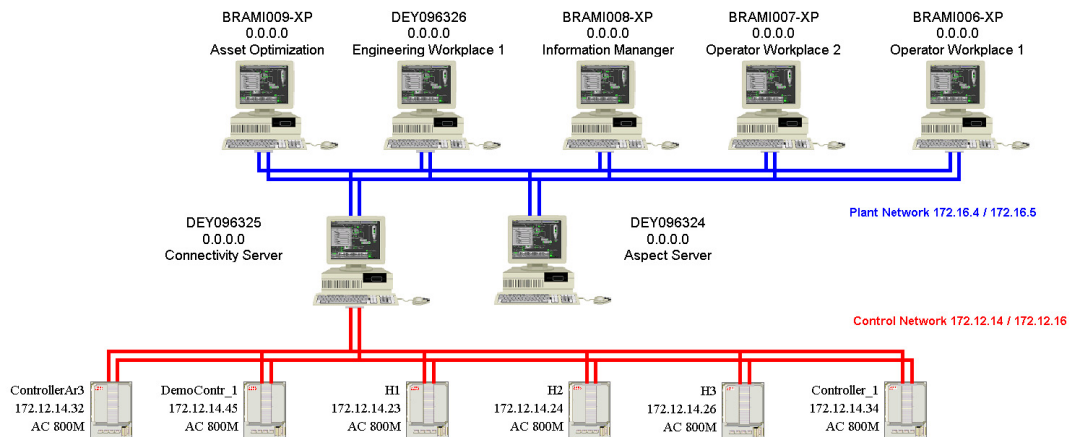


Figure 101. Topology Diagram over the Automation System Network

The Topology Designer and how to use it as Topology Status Viewer is described in *System 800xA Configuration (3BDS011222*)* and in *System 800xA Engineering, Engineering Studio Topology Designer (3BDS011225*)*.

Node Status Alarms

The network events that RNRP detects creates Node status alarms.

All node alarms have the following properties:

- The node object is used as the alarm source. The name of the node will be shown in the Object Name column in the alarm and event lists.
- The category used is “System Alarm for SoftAlarm”. This category is included in the System Alarms category group and the alarms will therefore show up in the default system alarm and event lists.

Node alarms are generated on some different alarm conditions:

- Network Connection Error. The message text includes the node name and the network area number where it has a problem. Note that a node may be connected to more than one area.

The following different sub conditions exist:

- Connection down. The node is not reachable at all.
- Primary network down. (The secondary is still OK.)
- Secondary Network down, (The Primary still OK.)

- Network Error Area <area no>. This condition describes the state of an entire network area. This condition occurs if the connection to all nodes on the network is lost, including the router nodes.

The following different sub conditions exist:

- Network down. The network is down.
- Primary network down. (The secondary is still OK.)
- Secondary Network down, (The Primary still OK.)



From the node alarm it is easy to navigate to the corresponding node object in the node administration structure via the objects context menu, see [Figure 98](#) on [page 232](#).

Alarms are only generated for nodes that are defined in the Node Administration Structure. For this reason Controllers are defined in both the Control Structure and in the Node Administration structure.



For the node status alarms to work properly Connectivity Servers, and possibly other nodes, that connect to both the Client/Server Network and the Control Network must use the same node number on both (all) Network Areas they are connected to.

Ping

Ping is a simple program for checking whether one node has contact with another node. Ping is available on all PCs. It is used from the Command prompt and its syntax is as follows: `drive:>ping address`

Example:

```
C:\>ping 172.16.0.201
```

Pinging 172.16.0.201 with 32 bytes of data:

```
Reply from 172.16.0.201: bytes=32 time<10ms TTL=64
Reply from 172.16.0.201: bytes=32 time<10ms TTL=64
Reply from 172.16.0.201: bytes=32 time<10ms TTL=64
Reply from 172.16.0.201: bytes=32 time<10ms TTL=64
```

Ping statistics for 172.16.0.201:

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

RNRP Network Monitor

In PCs where RNRP is installed there is a tool called the RNRP Network Monitor. When it starts up, it gives an overview of the entire network as seen from the node where it is running. For all nodes that are connected, it reports if there is a working connection between that node and the node where the Monitor is running. It shows if the connection is working on the primary or the secondary or both paths. After the initial overview all changes to the current status will be reported as for example **node up** and **node down** events.

The RNRP Network Monitor is started with a left-click on the **RNRP** icon in the Windows system tray.

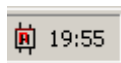


Figure 102. RNRP Icon in the System Tray

The RNRP icon is normally listed at **Start > All Programs > Startup** to be activated automatically when a user logs in. It can also be started by **Start > All Programs > ABB Industrial IT 800xA > System > Network > RNRP Create Icon**.

The RNRP Network Monitor can also be started at **Start > All Programs > ABB Industrial IT 800xA > System > Network > RNRP Monitor**.

```

RnrpMon Network Event Monitor
Monitor 3.3 connected to RnrpSvc 3.7 on SEABB-IS-11705.ATlab.local
RNRP Network Areas by distance:

!===== Network Area 1 ===== Distance 0 ===== Ethernet =====!
primary network (path0)= 172.16.4.0 ownNode= 1
secondary network (path1)= 172.17.4.0

4 reachable node(s)
-----
node= 2 paths=<up,up> ipa=<172.16.4.2 > h_name= SEABB-IS-11707.ATlab.local
node= 21 paths=<up,up> ipa=<172.16.4.21 > h_name= SEABB-IS-11704.ATlab.local
node= 71 paths=<up,up> ipa=<172.16.4.71 > h_name= SEABB-IS-11710.ATlab.local
node=401 paths=<up,up> ipa=<172.16.5.145 > type= WS

Primary Network ← Secondary Network

!===== Network Area 20 ===== Distance 1 ===== Ethernet =====!
primary network (path0)= 172.16.80.0 router(area,node)= 1, 21
secondary network (path1)= 172.17.80.0

1 reachable node(s)
-----
node= 21 paths=<up,up> ipa=<172.16.80.21 > name= SEABB-IS-11704.ATlab.local

-----
15/2 *16:53:16.034 Start waiting for events .....
  
```

Figure 103. RNRP Network Event Monitor with node names

Host names in the RNRP monitor

The RNRP monitor shows the node names for nodes where the RNRP's host file service works as intended (see [RNRP's host file service](#) on page 135). The names are displayed when the monitor is started.

Addresses for interface which are not registered in DNS will not be entered in the hosts file. An address which is entered in the hosts file is indicated with "h," before name = ... The figure above shows that the addresses on area 1 (172.16.4.x) are entered in the hosts file while the addresses on area 20 (172.16.80.21) are not entered. The node names are however shown also for these addresses (SEABB-IS11704.ATlab.local in the figure).

The figure also shows a node(172.16.5.145) for which the host file service does not work. The reason could be: that the other node run RNRP older than version 3.7 or that the Windows Firewall is misconfigured and blocks the name exchange communication.

AC 800M controllers do not support the host file service. For them the type field will indicate the Process Module type.

RNRP Events in Controllers

The same type of RNRP events that the RNRP Event Monitor can show can also be registered in the controller log in the standard AC 800M (but not in the AC 800M HI). These event messages are by default disabled, but they can be enabled by a method known to ABB's support organization.

The RNRP events may look like this in the controller log:

```
I 2004-10-01 16:04:31.128 RNRP: Node down, area=1 path=0 node=92
I 2004-10-01 16:05:03.631 RNRP: Node up, area=1 path=0 node=92
```

RNRP Fault Tracer/RNRP Utility

For a more detailed analysis of nodes using RNRP there is a tool called RNRP Fault Tracer. It is started with a right double-click on the RNRP icon in the system tray or

at **Start > All Programs > ABB Industrial IT 800xA > System > Network > RNRP Utility**.

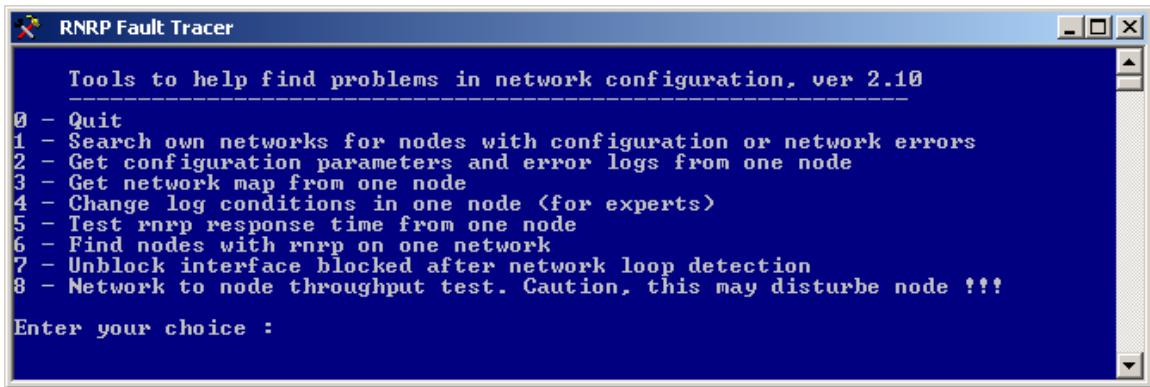


Figure 104. RNRP Fault Tracer/RNRP Utility

The RNRP Fault Tracer/RNRP Utility can:

- Check the RNRP configuration in a remote node.
- Ask a remote node about its view of the network (network map).
- Test response times between two nodes with RNRP ping.
- Find nodes using RNRP on one network independent of their configured area or IP addresses.
- Check for configuration errors in all reachable RNRP nodes on own network areas.
- Unblock blocked interfaces (see [RNRP Network Loop Detection and Protection](#) on page 72)

Network Interface Supervision in a PC

Windows representation of the network interfaces also provides some information about the status of the connections to the network. You start them via the **Network and Sharing Center > Manage Network Connections**. The status display for an interface is opened by a double-click on its icon.

Network Interface Supervision in a Controller

The status of the network interfaces in a controller is indicated in the hardware tree in the Control Builder when the Control Builder is in on-line mode, see [Figure 105](#). The indication **No communication** means that RNRP does not detect any nodes via that particular Network interface.

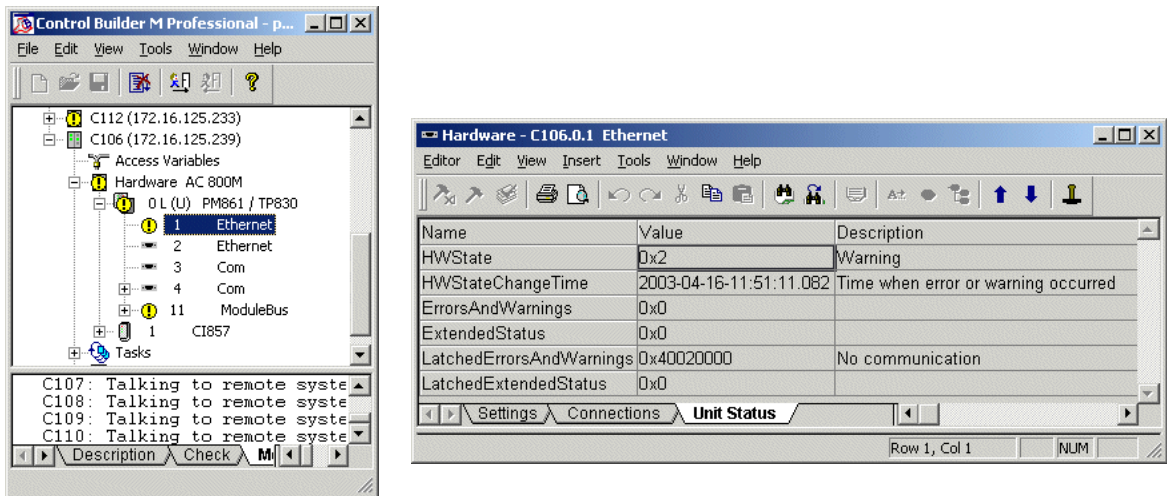


Figure 105. Network Interface Status in the Control Builder

The function block SystemDiagnostics, which by default is used in the Program3 when a controller application is created, contains a display about Ethernet statistics, see [Figure 106](#).

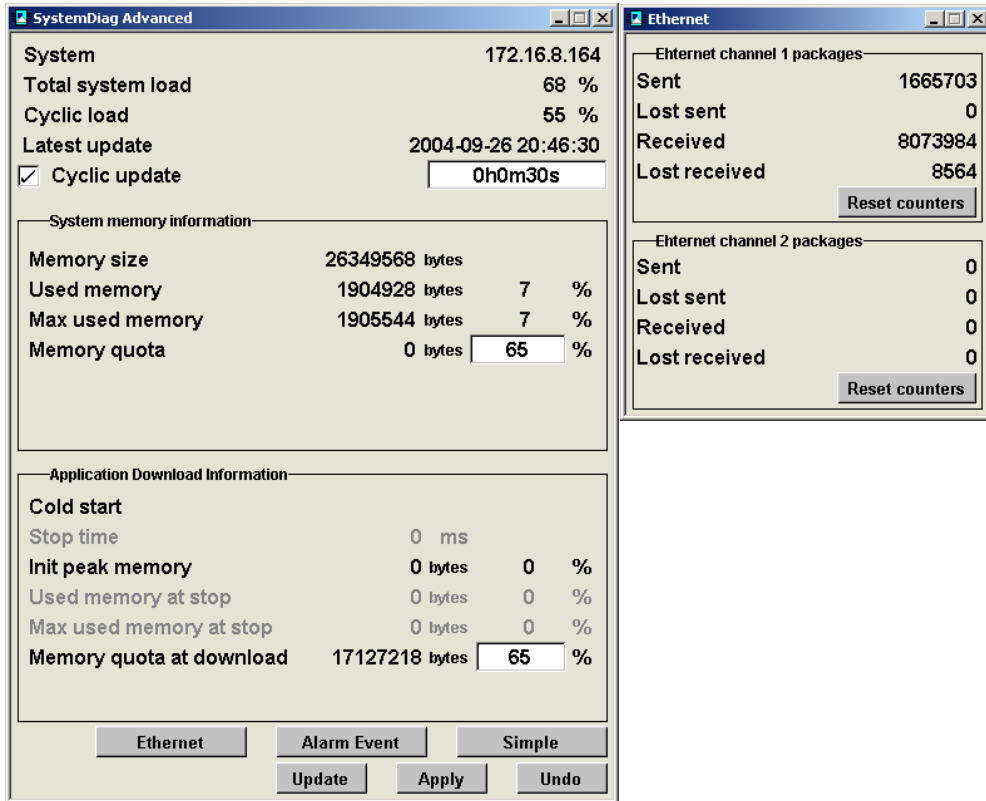


Figure 106. The Function Block SystemDiagnostics with Ethernet Statistics

Monitoring MMS Communication

The Control Builder includes a tool to supervise MMS connections to/from a node running MMS, see [Figure 107](#). The tool is started by right-clicking on the controller in the Control Builder Hardware tree, selecting Remote System, and clicking Show MMS Connections..

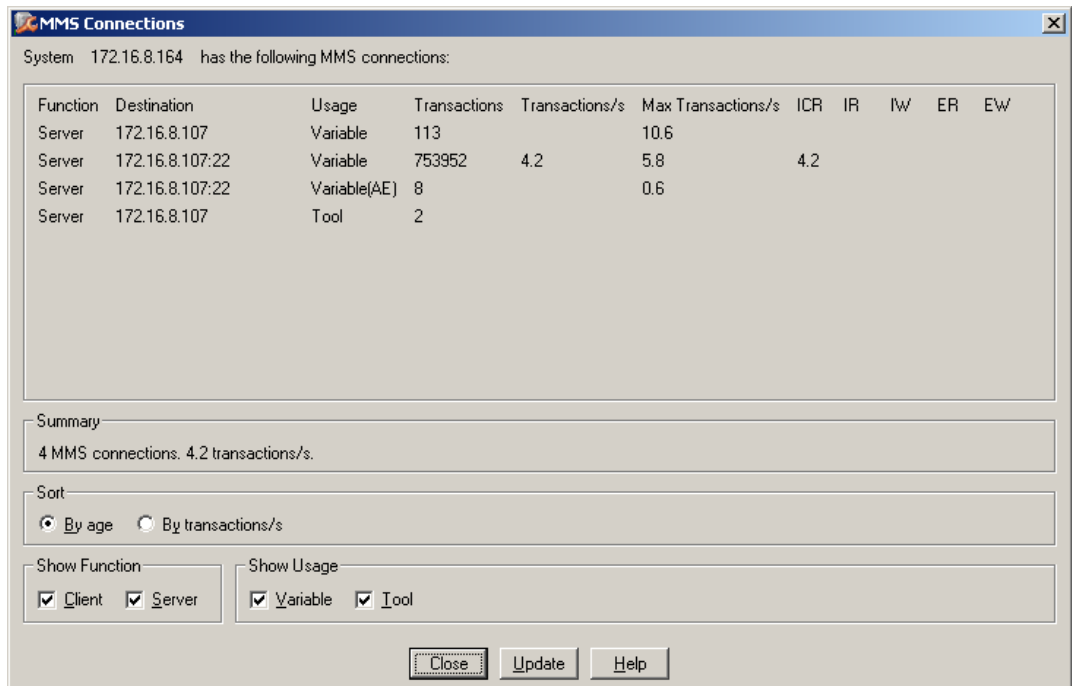


Figure 107. Show MMS Connections

The node may be a controller, an OPC server or a PC running the Control Builder. The OnLine help for the Control Builder describes more about what this viewer can show.

Using Network Management information

Switches that include network management can give information about the status of the network in general and specifically the status per network port, see [Features in Switches](#) on page 213.

Many switches provide built-in support for SNMP (Simple Network Management Protocol), which gives network management software the ability to monitor the health of the switch.

PC, Network and Software Monitoring

The 800xA System comes with a package called 'PC, Network and Software Monitoring' that can communicate via SNMP to device types (Assets) which support SNMP communications.

This allows switch health and status information to be shown in operator trends, graphics and logs, as well as incorporated into the standard System Status Viewer Aspect. The System Status Viewer will show the first error encountered for an Asset, as seen in [Figure 108](#).

Objects	Status	Time	Description	Detail
IT Server, IT OPC Server Network				
brahms2, Generic Computer Node	✘	2004-08-30 23:21:57	General Computer Alarm-VM-T...	X
IM Calc, Inform IT Calculations	✘	2004-08-25 16:19:54	CalculationServer.exe Alarm-Pr...	X
Lab Printer, Generic Printer Node	✘	2004-08-30 11:09:25	Printer Alarm-LowPaper	X
Shadow9 Network, Network Utilization	●	2004-08-26 16:14:39	OK	X
Shadow9, Generic Computer Node	✘	2004-08-30 23:21:35	General Computer Alarm-VM-T...	X
Switch #236 (East Plant Network), Hirs	✘	2004-08-31 08:47:54	Hirschmann Alarm-Port-1	X

Figure 108. System Status Viewer showing Error on Port 1

The package contains faceplates that visualize status information from different device types.

Figure 109 shows the faceplate for a Hirschmann RS2 switch. In this example the faceplate shows under the Operating Status column that there is no cable attached for Interface Indexes 1,2,3,6,7.

Interface Index	Operating Status	Media Available	Total Input	Total Output	Media Speed (Mbps)
1	down	notAvailable	0	200	0
2	down	notAvailable	0	64	0
3	down	notAvailable	0	64	0
4	up	available	2636713499	1036013563	100
5	up	available	64239619	1756604180	10
6	down	notAvailable	0	132	0
7	down	notAvailable	0	200	0

Figure 109. Faceplate for a Switch with SNMP Support

When combined with the 800xA Asset Optimization functionality, the system can automatically detect problems and generate alarms based on this information as seen in Figure 110.

Severity	AM Name	Condition	SubCondition	Description	TimeStamp	QualityStatus
1	IT Asset Monitor	Hirschmann Alarm:PowerSupply-1	Normal	OK	2004-08-31 08:48:22	good
1	IT Asset Monitor	Hirschmann Alarm:PowerSupply-2	Normal	OK	2004-08-31 08:48:22	good
500	IT Asset Monitor	Hirschmann Alarm:Port1	Unconnected	Port is unconnected	2004-08-31 08:48:22	good
500	IT Asset Monitor	Hirschmann Alarm:Port-2	Unconnected	Port is unconnected	2004-08-31 08:48:22	good
500	IT Asset Monitor	Hirschmann Alarm:Port-3	Unconnected	Port is unconnected	2004-08-31 08:48:22	good
1	IT Asset Monitor	Hirschmann Alarm:Port-4	Normal	OK	2004-08-31 08:48:22	good
1	IT Asset Monitor	Hirschmann Alarm:Port-5	Normal	OK	2004-08-31 08:48:22	good
500	IT Asset Monitor	Hirschmann Alarm:Port-6	Unconnected	Port is unconnected	2004-08-31 08:48:22	good
500	IT Asset Monitor	Hirschmann Alarm:Port-7	Unconnected	Port is unconnected	2004-08-31 08:48:22	good

Figure 110. Asset Optimization Asset Reporter showing no Cable attached on some Ports

Please refer to *System 800xA Configuration (3BDS011222*)* for more details on how to configure this package.

Network Management Tools from Switch Vendors

Vendors of switches with network management information also supply tools that can show and manipulate this information. There are many tools for accessing SNMP data. Many network switches include web servers. In this case only a web browser is needed to access the information in the switch. Some vendors also supply OPC servers for their switches so that the network management information is available to use for OPC clients. This means that the network management information is possible to access from the 800xA System as from any third party OPC servers.

Appendix A Reference Details

This appendix section describes the reference details used in the nodes.

IP Addresses



It is strongly recommended that the addresses presented in, [Recommended IP Address Plan](#) on page 30, are used. If they are used, no extra RNRP configuration is required and the following chapter about addressing may be ignored.

All nodes in the Industrial^{IT} System networks are identified by their IP Address. IP stands for Internet Protocol. The IP address is a 32-bit word (4×8 bits) that often is written in the form X.Y.Z.Q with four decimal numbers 0-255, separated by periods.

The IP standard uses the terms *NetID* and *HostID*. The *subnet mask* specifies the boundary between the NetID part and the HostID part of the IP address (the zero bits indicate the HostID part). A (part of a) network where all nodes use the same NetID is called a subnet.

Depending on the value of X, IP addresses are divided mainly into three classes, A–C:

Table 47. IP Address Classes

IP address in bit format		XXXXXXXX.YYYYYYYY.ZZZZZZZZ.QQQQQQQQ			
Class A		←NetID→	←HostID→		
Class B		←NetID→		←HostID→	
Class C		←NetID→			
Class	Value of X	NetID	HostID	Possible host IP addresses	Default subnet mask
A	1-126	X	Y.Z.Q	X.0.0.1-X.255.255.254	255.0.0.0
B	128-191	X.Y	Z.Q	X.Y.0.1-X.Y.255.254	255.255.0.0
C	192-223	X.Y.Z	Q	X.Y.Z.1-X.Y.Z.254	255.255.255.0

Example with 24 bit NetID and 8 bit HostID:

```
IP Address: 192. 16. 10.56
Address mask:255.255.255. 0
NetID:      192. 16. 10.
HostID :                    56
```

The boundary between NetID and HostID does however not need to be at even byte-boundaries.

Example with 22 bit NetID and 10 bit HostID:

```
IP Address: 172. 16. 5.101
Address mask:255.255.252. 0
NetID:      172. 16. 4.
HostID :                    1.101 (=256+101=357)
```

The 3:rd byte (=5) contains bits from both NetID and HostID.

What happens with the 2 last bytes is perhaps more clear in the binary notation:

```
IP Address5. 101    = 0000 0101 0110 0101
Address mask252.0 = 1111 1100 0000 0000
```



```

NetID:    4.    0    = 0000 0100 0000 0000
HostID :  1. 101    = 0000 0001 0110 0101

```

The address mask 255.255.252.0 is chosen for implicit RNRP configuration. This is described in section [Address Rules for Implicit RNRP Configuration](#) on page 52.

A common way to write an IP address including the information about the address mask is X.Y.Z.Q/H. Where H is the number of bits in the NetID. The 2:nd example above would be written 172.16.5.101/22.

How to Choose IP Addresses

The user must plan what IP addresses to use for all nodes in the system.

Choosing Address Space

The first thing to choose is the address space for the network. It is recommended to use private addresses. This has the following advantages:

- There is no requirement to apply to the licensing authorities for an IP address, i.e. it is easy to allocate a large IP address space.
- Some protection is gained against illegal access, because private addresses are not permitted on the public Internet.

The following private addresses may be selected as “Default Network ID”¹ when using implicit RNRP configuration:

IP Class A addresses:

10. n*4. 0. 0 n= 0, 1, 2, , , , ,63

IP Class B addresses:

172. 16. 0. 0

172. 20. 0. 0

172. 24. 0. 0

172. 28. 0. 0

1. See [RNRP Configuration Parameters](#) on page 54

Using Implicit or Explicit RNRP Configuration

To simplify the configuration of RNRP it is recommended to use implicit RNRP configuration. Explicit RNRP configuration must on the whole only be used if the user has their own requirements on the network that do not allow implicit RNRP configuration. The following criteria decide whether Implicit RNRP Configuration can be used:

- A private address space with one of the Default Network IDs as described in the previous section or the chosen address range anyway complies to the following criteria:
 - There are 2 complete Class A or B networks (one for nonredundant) $N_1.N_2.0.0$ (and $N_1.(N_2+1).0.0$) where N_2 is an even multiple of 4.
 - All addresses from $N_1.N_2.0.0$ to $N_1.(N_2+1).255.255$ are free to use.
- The Address Mask must be 255.255.252.0
- The following configuration parameters (see [Table 47](#)) must be the same for all network interfaces in the node:
 - Network Base Address
 - Send Period
 - Max number of lost messages

Using the implicit method has the following advantages compared to the explicit:

- Less manual configuration work has to be done.
- It decreases the risk of inconsistent configuration.
- If the default values for the configuration parameters can be used, NO manual configuration of RNRP is necessary in the node. It is sufficient to configure the IP address and the Address Mask.

With the Explicit Configuration method, specific RNRP configuration has to be done in each node, in addition to the configuration of IP address and subnet mask, even if many parameters can use default values.

An example of using the explicit method is in a node with both connections to the normal Ethernet based Control Network and to a PPP link, since it is recommended to use a Send Period greater than the default value for PPP links.

To use implicit RNRP configuration do as follows for each node:

1. Decide the RNRP address parameters.
2. Calculate the IP address based on the RNRP address parameters using one of the formulas in [Address Rules for Implicit RNRP Configuration](#) on page 52. Set the IP address and the Address Mask per interface. (RNRP extracts the RNRP address parameters from the IP address)

To use the explicit address selection method do as follows for each node:

1. Decide the IP addresses.
2. Decide the RNRP address parameters.
3. Set the parameter “number of explicit addresses” to cover the appropriate number of network interfaces.
4. Set the IP address and the Address Mask for each network interface.
5. Set the RNRP address parameters for each network interface.

Suggested Configuration of RNRP and IP Addresses

Below are some principles to follow when choosing the addresses.

There are no requirements on what addresses to set on what nodes in the system, but these are some suggestions of how to organize the network:

- Use addresses that allow implicit RNRP configuration if possible¹ (see [RNRP Address Configuration: Implicit or Explicit](#) on page 50). Use the private base address 172.16.0.0 if possible (see [Choosing Address Space](#) on page 249).
- Define address groups for similar types of nodes used in the system. Define these groups with spare addresses for future extensions of the system. Use the same group definitions on all network areas, e.g. let node number 101 always be reserved for a Workplace Client and 201 for a Controller.

1. “If possible” means “if the user does not have any contradicting requirements on the network” e.g. using PPP.

- Nodes that connect to several Network Areas (typically Connectivity Servers) must use the same Node number on the different networks.
- Use the default rule for the address of Backup Controllers (see [IP Addresses for Redundant Controller Nodes](#) on page 252).
- For systems where it is unlikely that there will be more than 256 nodes, use node numbers less than 256. This way the last byte in the IP address will correspond to the node number.
([Address Rules for Implicit RNRP Configuration](#) on page 52 describes how to calculate IP addresses based on RNRP parameters.)

IP Addresses for Redundant Controller Nodes

All nodes on the network need a unique IP address. This is true also for all nodes with unit redundancy like for example redundant servers or controllers with CPU redundancy.

In case of redundant servers each node always has its own IP address. There is no special rule about how to choose the addresses for the redundant servers.

In case of redundant AC 800M controllers the Primary CPU always works with the primary IP addresses. In case of a switch-over, the addresses are also switched. The addresses of the Backup CPU can be configured arbitrarily, but to simplify the configuration there is a default rule for it:

The default addresses of a Backup CPU is the same addresses as the backup except that: $\text{BackupNodeNumber} = \text{PrimaryNodeNumber} + 512$.

Note that this is an exception to the rule that node numbers can not be higher than 500.

Byte wise this means that if the address of the Primary is A.B.C.D the address of the Backup is: A.B.C+2.D

Index

Numerics

- 800xA for AC 800M 156
- 800xA for AC 800M Time Adaptor 146
- 800xA for Advant Master 156
- 800xA for Harmony 156
 - Adjusting Time 206
 - Clock Sync 192
 - SettingTime 206
- 800xA for Melody 156
 - Adjusting Time 206
 - Clock Sync 193
 - Setting Time 206

A

- Adapters and Bindings 138
- Address Space 249
- AfwTime 198
- AfwTime Client 186
- AfwTime Server 184
- AfwTime Service 180
 - Local Time Service 146
- Allowed to Set Time 187
- Aspect Server 140

B

- Backup CPU 141, 252
- Base Address 52

C

- Cable Color 227
- CAT5 217
- CI855 160, 164
- Class A 248
- Class B 248
- Class C 248

- Client/Server Network 23
- Clients allowed to set Time 183
- CLK_MAST 190
- CLK_SEND 190
- CLOCK_SYNCH 174, 190
- CNCP 174
- Communication
 - Broadcast 38
 - Multicast 38
- Connectivity Server 141
 - as Routers 42
 - using RNRP 26
- Control Network 23
- CPU Redundancy 229, 252
- CS CNCP ClockMasterOrderNo 172
- CS Protocol Type 172
- CS SNTP ServerAddr1 172
- CS SNTP ServerAddr2 172
- CS Synch Interval 172
- CS Time Set Enabled 172, 202

D

- Data Recover Time 41
- Daylight Saving Time 196
 - Support 196
- Defense in depth 92
- DNS 139
 - Configuration 132, 142
 - Introduction 36
 - Parameters 125
 - Server 129
- Domain Controllers 123, 197
 - Introduction 35
- Domain Name 123
- Duplex 215

- E**
 - Ethernet 211
- F**
 - Fault Handling 40
 - Firewalls 94
 - Application Proxies 95
 - Packet Filtering 94
 - Stateful Inspection 95
 - flushdns 143
- G**
 - GPS 176
 - GPS Receiver 150
- H**
 - Hop Count 42, 45
 - HostID 247
 - HostID Part 50
 - Hubs 212
- I**
 - IGMP Snooping 214
 - Interface Status 240
 - Internet Protocol 247
 - IP Address 50, 247
 - IP Address Plan 30
 - IP Routers 62
 - ipconfig 143
 - IPSec 67
- L**
 - Layer 2 VPN 66
 - Layer 3 VPN 67
 - LOC_TIME 190
 - Local Network Area 47
 - Local Time Source 146
- M**
 - MaxLostMessages 41
 - MB 300 160
 - as Clock Master 164
 - Clock Synchronization 178
 - via CI855 173
 - MMS Time Synchronization 180
 - MPLS 66
 - Multi-mode fiber 225
- N**
 - NetBIOS 123
 - NetID 247
 - NetID part 50
 - NetRemoteTOD 183
 - Network Address Translation (NAT). 96
 - Network Area 38
 - Network Area Number 39
 - Network Areas 24
 - Network Fail over Time 40
 - Network Interfaces 137
 - Network Redundancy 37
 - Introduction 28
 - Primary Network 28
 - Secondary Network 28
 - Network Security 91
 - Network Segment 212
 - Node Administration structure 231
 - Node down 237
 - Node Number 39
 - Node up 237
- O**
 - OPC Server 180, 215
- P**
 - Path Number 38
 - Ping 237
 - Plant Network 23
 - PPP 28

Primary CPU 252
Private Address Space 29
Private Addresses 249

Q

Quality of Service 215

R

Redundant Controller 252
registerdns 143
Ring Redundancy 220
RJ-45 216
RMON 215
RNRP 37
 Base Parameters 55
 Explicit Parameters 59
 Network Monitor 70, 237
 Tunnel Areas 62
RNRP Configuration
 Implicit 51
RNRP icon 237
Router
 Redundant 44
Routers 230
RTA Board 174
 Clock Synchronization 190

S

Send Period 40
Server Group 184
Server running 183
Service Handler 180
Service Provider 180
SetDT 204
Shielded Twisted Pair (STP) 216
SNMP 215
 Network Management 244
SNTP 176
SNTP Server 150, 196
Spanning Tree 215

Store-and-forward delay 213
STP Cable 224
Subnet Mask 247
Switches 212
System Status Providers 231
System Status Viewer 231, 244

T

TCP/IP Forwarding 69
Time Adaptor
 AC 800M 189
 Advant Master 189
Time Adaptors 188
Time Client 180
Time Server 180
Time Set 202
Time Synch Running 187
TimeServerHandler
 Aspect 186
Trusted Network Zones 92
TSP 192

W

W32Time 198, 205
w32tm 205
WAN 61
Windows system tray 237
Windows Time Service 177, 194 to 195, 197

Revision History

This section provides information on the revision history of this User Manual.



The revision index of this User Manual is not related to the 800xA 5.1 System Revision.

The following table lists the revision history of this User Manual.

Revision Index	Description	Date
-	First version published for 800xA 5.1	June 2010
A	Updated for 800xA 5.1 Rev A	May 2011
B	Updated for 800xA 5.1 (64-bit)	December 2011
C	Updated for 800xA 5.1 FP2 (32-bit)	December 2011
D	Updated for 800xA 5.1 FP3 release	August 2012
E	Updated for 800xA 5.1 FP4 release	February 2013

Updates in Revision Index A

The following table shows the updates made in this User Manual for 800xA 5.1 Rev A.

Updated Section/Subsection	Description of Update
Section 1, Introduction	Updated the Recommended IP Address Plan sub-section.
Section 2, Network Redundancy and Routing	Updated the Building large networks by using Backbone Network Areas sub-section.
Section 8, Ethernet and Network Equipment	Updated the Coexistence of Network Types sub-section.

Updates in Revision Index B

The following table shows the updates made in this User Manual for 800xA 5.1 (64-bit).

Updated Section/Subsection	Description of Update
Section 7, Time Synchronization	Updated the SNTP Server addresses in the Tables and in the subsection Configure Time Synchronization in a Dedicated Domain Controller.

Updates in Revision Index C

The following table shows the updates made in this User Manual for 800xA 5.1 Feature Pack 2 (32-bit).

Updated Section/Subsection	Description of Update
About this User Manual	Added a new sub-section Feature Pack.
Section 2 Network Redundancy and Routing	Updated content for RNRP Network Loop Detection and Protection sub-section.

Updated Section/Subsection	Description of Update
Section 5 Network Security	Added a new sub-section AC 800M Network Storm Protection.
Section 7 Time Synchronization	Updated the content in Advant Master Time Adaptor sub-section.

Updates in Revision Index D

The following table shows the updates made in this User Manual for 800xA 5.1 Feature Pack 3.

Updated Section/Subsection	Description of Update
Section 2 Network Redundancy and Routing	Removed the FP icons for RNRP Network Loop Detection and Protection sub-section. Changes done in the Control Network subsection.
Section 5 Network Security	Removed the FP icons for AC 800M Network Storm Protection.
Section 7 Time Synchronization	Removed the FP icons for the content in the Advant Master Time Adaptor sub-section.
Section 3 Distributed System Topologies	Added Asset Optimization subsection in the Multisystem Integration section.

Updates in Revision Index E

The following table shows the updates made in this User Manual for 800xA 5.1 Feature Pack 4.

Updated Section/Subsection	Description of Update
About this User Manual	Changes done in the table.
Section 1. Introduction	Changes done in the following subsection: <ul style="list-style-type: none">• Control Network• Large Configuration with Control Network on Two Network Areas• Introduction to DNS, Name and Address resolution
Section 2. Network Redundancy and Routing	Changes done in the following subsection: <ul style="list-style-type: none">• RNRP• Multiple Network Areas and RNRP Routers• Special Routing Consideration• RNRP Configuration Parameters• Use of Layer 2 VPN Solutions• Building large networks by using Backbone Network Areas
Section 8. Ethernet and Network Equipment	Changes done in the Ethernet Speed subsection.
Section 6. Domain Setup and Name Handling	Changes done in the RNRP's host file service subsection.

Contact us

ABB AB

Control Technologies

Västerås, Sweden

Phone: +46 (0) 21 32 50 00

e-mail: processautomation@se.abb.com

www.abb.com/controlsystems

ABB Automation GmbH

Control Technologies

Mannheim, Germany

Phone: +49 1805 26 67 76

e-mail: marketing.control-products@de.abb.com

www.abb.de/controlsystems

ABB S.P.A.

Control Technologies

Sesto San Giovanni (MI), Italy

Phone: +39 02 24147 555

e-mail: controlsystems@it.abb.com

www.abb.it/controlsystems

ABB Inc.

Control Technologies

Wickliffe, Ohio, USA

Phone: +1 440 585 8500

e-mail: industrialitsolutions@us.abb.com

www.abb.com/controlsystems

ABB Pte Ltd

Control Technologies

Singapore

Phone: +65 6776 5711

e-mail: processautomation@sg.abb.com

www.abb.com/controlsystems

ABB Automation LLC

Control Technologies

Abu Dhabi, United Arab Emirates

Phone: +971 (0) 2 4938 000

e-mail: processautomation@ae.abb.com

www.abb.com/controlsystems

ABB China Ltd

Control Technologies

Beijing, China

Phone: +86 (0) 10 84566688-2193

www.abb.com/controlsystems

Copyright © 2003-2013 by ABB.

All rights reserved.

3BSE034463-510 E

Power and productivity
for a better world™

