

Experion PKS  
Fault Tolerant Ethernet Overview and  
Implementation Guide

EPDOC-XX37-en-431A  
February 2015

**Release 431**

Document	Release	Issue	Date
EPDOC-XX37-en-431A	431	0	February 2015

## Disclaimer

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Sàrl.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Copyright 2015 - Honeywell International Sàrl

# Contents

<b>1 Introduction .....</b>	<b>7</b>
1.1 About this document .....	8
1.1.1 Typical users of this document .....	8
1.1.2 Acronyms and abbreviations .....	8
1.1.3 FTE specific terms and definitions .....	9
1.2 Fault Tolerant Ethernet (FTE) functional overview .....	10
1.2.1 Functional Overview .....	10
1.2.2 Communication between FTE nodes .....	10
1.2.3 Fault recovery information .....	11
1.2.4 Using FTE with existing systems .....	11
1.2.5 FTE transmission support .....	11
1.3 FTE network overview .....	12
1.3.1 FTE community .....	12
1.3.2 FTE tree .....	13
1.3.3 FTE groupings and switch pairs .....	13
1.3.4 FTE nodes .....	13
1.3.5 FTE media components .....	14
<b>2 Planning a Honeywell network .....</b>	<b>15</b>
2.1 Before you begin .....	16
2.1.1 Assumptions .....	16
2.1.2 Network services consulting and support for FTE .....	16
2.1.3 Planning an FTE network .....	16
2.2 FTE network infrastructure .....	17
2.2.1 Plant network levels .....	17
2.2.2 FTE community .....	17
2.2.3 Maximum nodes within an FTE community .....	17
2.2.4 Large FTE systems .....	17
2.3 FTE best practices summary .....	19
2.3.1 FTE critical configuration items .....	19
<b>3 Level 1 nodes .....</b>	<b>21</b>
3.1 About level 1 nodes .....	22
3.1.1 Series C Level 1 LAN cluster .....	22
3.2 Level 1 best practices .....	23
3.2.1 Honeywell Control Firewall best practices .....	23
3.2.2 Honeywell Control Firewall features .....	23
3.2.3 C200 with FTEB best practice .....	23
3.2.4 Series A Level 1 LAN cluster .....	24
3.2.5 Connecting Level 1 LAN clusters .....	24
3.2.6 Connecting Level 1 nodes that intercommunicate .....	25
3.2.7 Using a switch for level 1 and level 2 (split switch configuration) .....	25
<b>4 Level 2 nodes .....</b>	<b>27</b>
4.1 About level 2 nodes .....	28
4.1.1 Level 2 LAN .....	28
4.2 Level 2 Best Practices .....	29
4.2.1 Configuring level 2 switch .....	29

4.2.2	Avoiding multiple network connections .....	29
4.2.3	Non FTE dual attached nodes within level 2 .....	29
4.2.4	Non FTE single attached nodes within level 2 .....	29
4.2.5	Nodes with embedded operating systems .....	29
4.2.6	Critical nodes .....	30
4.2.7	Best practices for connecting a crossover cable .....	30
4.3	Implementing level 2 best practices .....	31
4.3.1	Separate IP address range .....	31
4.3.2	Using filters in level 3 routers .....	31
4.3.3	Domain controllers in an FTE network .....	31
4.3.4	Connecting level 2 to level 1 .....	32
4.4	Safety Controller Best Practices .....	33
4.4.1	Systems with peer-to-peer control communication .....	33
4.4.2	Systems using SCADA data only .....	33
<b>5</b>	<b>Level 3 nodes .....</b>	<b>35</b>
5.1	About level 3 nodes .....	36
5.1.1	Level 3 LAN .....	36
5.2	Level 3 best practices .....	37
5.2.1	Implementing Level 3 best practices .....	37
5.2.2	Using Redirection Manager (RDM) with Level 3 .....	37
5.3	Level 2 to level 3 best practices .....	38
5.3.1	Best practice for multiple connections from level 2 to level 3 .....	38
5.3.2	Connecting level 2 to level 3 .....	38
5.3.3	View of level 2 from level 3 with router and filter .....	39
<b>6</b>	<b>Level 4 nodes .....</b>	<b>41</b>
6.1	About level 4 nodes .....	42
6.1.1	Process control network to business network .....	42
6.2	Level 4 best practices .....	43
6.3	Implementing Level 4 Best Practices .....	44
6.3.1	Firewall requirements .....	44
6.3.2	Router configuration .....	44
6.3.3	Firewall requirements .....	44
6.3.4	Establishing a DMZ .....	44
6.3.5	Recommended communication restrictions .....	45
<b>7</b>	<b>Additional Best Practices .....</b>	<b>47</b>
7.1	Robust FTEB-based topology .....	48
7.1.1	Configuration rules for a robust topology .....	48
7.1.2	FTEB switch connection guidelines for critical process .....	48
7.1.3	FTEB switch connection guidelines for non-critical processes .....	48
7.1.4	OneWireless best practices .....	48
7.1.5	PCDI best practices .....	48
7.2	Variations on Best Practice .....	49
7.2.1	Remote locations .....	49
7.2.2	System with station on split switches .....	49
7.2.3	Split switch configuration .....	50
7.2.4	Small Experion systems with FTE .....	50
7.2.5	Third-party safety equipment .....	51
7.3	Digital video manager best practices .....	52
7.4	TPS upgrade best practices .....	53
7.4.1	Connecting TPS nodes to the FTE network .....	53
<b>8</b>	<b>Use of IP Addresses in an FTE Network .....</b>	<b>55</b>
8.1	Introduction .....	56

8.1.1	IP address ranges for FTE communities .....	56
8.1.2	IP address range selection recommendations .....	56
8.1.3	IP addresses for non-Honeywell nodes .....	57
8.1.4	Duplicate IP addresses .....	57
8.1.5	Best practices for preventing duplicate IP addresses .....	57
8.1.6	Recovering from a communication loss due to a duplicate IP address .....	57
8.2	Recommendations for FTE Network Communities .....	59
8.2.1	Isolated FTE community .....	59
8.2.2	Multiple FTE communities isolated from Level 4 networks .....	59
8.2.3	FTE Communities connected to Level 4 with NO COM communications .....	59
8.2.4	Private address distribution ranges .....	59
8.2.5	FTE communities connected to level 4 with COM communications .....	60
8.3	Reusing IP Addresses for Level 1 .....	62
8.3.1	Purpose .....	62
8.3.2	Address reuse scheme for level 1 .....	62
8.3.3	Route add command .....	62
8.3.4	Interface metric for non-FTE nodes .....	63
<b>9</b>	<b>Installing and Replacing Switches .....</b>	<b>65</b>
9.1	Introduction .....	66
9.1.1	Prerequisites .....	66
9.1.2	Qualified network equipment for use in an FTE network .....	66
9.2	Installing and Configuring Cisco Switches .....	67
9.2.1	FTE switch installation guidelines .....	67
9.2.2	Configuring Cisco switches to prevent storms .....	67
9.2.3	Expanding an existing FTE network .....	67
9.2.4	Using spanning tree .....	68
9.2.5	Ciscoswitch port and connection speeds .....	68
9.3	Replacing Switches .....	70
9.3.1	Upgrading the switch .....	70
9.3.2	Guidelines for replacing FTE switches .....	70
9.3.3	Special considerations for replacing stacked switches .....	70
9.3.4	Tasks for configuring and replacing switches .....	70
9.4	Stacking Switches .....	72
9.4.1	About stacked switches .....	72
9.4.2	Tasks for stacking switches .....	72
9.4.3	Checking the switch IOS .....	73
9.4.4	Modifying the stacked switch configuration files .....	74
9.4.5	Configuring switch priority in a stacked switch .....	75
9.5	Honeywell control firewall .....	76
9.5.1	Honeywell control firewall connection requirements .....	76
9.5.2	Honeywell control firewall guidelines .....	76
9.5.3	Benefits of Honeywell control firewalls .....	77
9.6	Honeywell's switch configuration files .....	78
9.6.1	Location of switch configuration files .....	78
9.6.2	Obtaining the latest switch configuration files .....	78
9.6.3	Switch configuration requirements .....	79
9.6.4	Configuring switches for network level communication .....	79
9.6.5	Cisco switch and port options .....	81
9.6.6	Configuration order for switch ports .....	81
9.6.7	Switch configuration examples .....	81
9.6.8	Details for switch configuration files .....	83
9.7	Configuring Cisco switches .....	89
9.7.1	Before you begin .....	89
9.7.2	Passwords and names for switch access and configuration .....	89

9.7.3	Tasks for configuring a Cisco switch .....	90
9.7.4	Accessing switch configuration files .....	90
9.7.5	Connecting locally to the switch .....	91
9.7.6	Configuring switch interface options .....	92
9.7.7	Using VLAN101 switch configuration files .....	98
9.7.8	Loading the switch configuration file .....	98
9.8	Saving and modifying Cisco switch configuration files .....	103
9.8.1	Downloading the switch configuration file (optional) .....	103
9.8.2	Enabling Telnet on your system .....	104
9.9	Updating the Honeywell control firewall firmware .....	105
9.9.1	Firewall devices .....	105
9.9.2	Determining necessity of firmware update .....	105
9.9.3	Firewall firmware update process .....	105
9.9.4	Before using the control firewall update tool .....	106
9.9.5	Launch the control firewall update tool .....	106
<b>10</b>	<b>Configuring a switch for SSH .....</b>	<b>107</b>
10.1	Configuring Cisco switch for SSH .....	108
10.2	Using Tera Term for SSH Communications .....	110
<b>11</b>	<b>Troubleshooting Network Issues .....</b>	<b>113</b>
11.1	Preventing Crosslink Errors .....	114
11.1.1	FTE diagnostic messages .....	114
11.1.2	Definition of crosslink error .....	114
11.1.3	Potential causes of crosslink errors .....	114
11.2	Intermittent or blocked communication to controllers on a different subnet .....	116
11.3	Mismatch of FTE multicast address and destination port .....	117
<b>12</b>	<b>Switch and Router Configuration Examples .....</b>	<b>119</b>
12.1	Cisco switch and router examples .....	120
12.2	Cisco router configuration statements .....	121
12.2.1	Access control lists .....	121
12.2.2	Cisco 3560, 2960, IE3000 access list for protecting Safety Manager or third-party safety controllers .....	122
12.3	Subnet mask derivation .....	123
12.4	Stacked switch configuration examples .....	124
12.4.1	Single domain controller with a 100 mb or CF9 connection .....	124
12.4.2	Uplink to 100 mb switch connection on switch 1, port 12 .....	124
<b>13</b>	<b>Notices .....</b>	<b>125</b>
13.1	Documentation feedback .....	126
13.2	How to report a security vulnerability .....	127
13.3	Support .....	128
13.4	Training classes .....	129

# 1 Introduction

## **Related topics**

“About this document” on page 8

“Fault Tolerant Ethernet (FTE) functional overview” on page 10

“FTE network overview” on page 12

## 1.1 About this document

This guide contains basic installation instructions and configuration requirements for an FTE network and its components. Detailed network planning and requirements information is not included as this type of information is site-specific.

### Revision history

Revision	Date	Description
A	February 2015	Initial release of the document.

### 1.1.1 Typical users of this document

It is assumed that the user performing FTE network installation is familiar with networking fundamentals.

Typical users of this guide include.

- Network administrators
- System administrators
- Project planners
- FTE network users

### 1.1.2 Acronyms and abbreviations

Acronym	Description
ACE	Advanced Control Environment- An Experion node used for high-level control.
ACL	Access Control List - A Cisco command for filtering traffic.
CDA	Control Data Access - The Experion data access layer.
COM	Component object model.
ControlNet	A Rockwell communication protocol.
DC	Domain Controller.
DHEB	Data Hiway Ethernet Bridge.
DSA	Distributed System Architecture - The Experion method of sharing data.
FIM	Fieldbus Interface Module.
FTE	Fault Tolerant Ethernet - the control network of Experion.
FTEB	Fault Tolerant Ethernet Bridge - The communications bridge between FTE and ControlNet.
GBIC	GigaBit Interface Converter module for Cisco switches.
IP	Internet Protocol.
LAN	Local Area Network.
LDAP	Lightweight Directory Access Protocol - a client-server protocol for accessing a directory service.
MAC	Media Access Controller.
NAT	Network Address Translation.
NetBIOS	Network Basic Input/Output System.
NIC	Network Interface Controller.
PHD	Process History Database - The Experion history node.



Acronym	Description
PIN	Plant Information Network.
STP	Shielded Twisted Pair.
TCP	Transport Control Protocol.
Uplink	Any interface that connects switches to switches or switches to routers.
FTEMux	FTEMux is the version of the FTE driver designed for NDIS 6.0 (Windows Vista, Windows 7 and Windows Server 2008 operating systems). It provides FTE functionality, compatible with previous releases, with a single TCP/IP stack (Only 1 IP address required) on a virtual adapter.

### 1.1.3 FTE specific terms and definitions

The following terms and definitions associated with FTE are used throughout this guide in the following context.

Term	Definition
FTE Node	FTE Nodes are those with the necessary redundant media components and Honeywell FTE software.
FTE Grouping	A collection of nodes associated with the same process unit. That is, a server, stations, and controllers, which typically have high intercommunication.
FTE Community	A group of FTE and non-FTE nodes within the same broadcast domain.
Yellow	For FTE, refers to all the components connected to the primary A switch, each of which is usually connected using the Honeywell-provided yellow cables.
Green	For FTE, refers to all the components connected to the secondary B switch, each of which is usually connected using the Honeywell-provided green cables.
FTE Tree	FTE topology is two parallel tree hierarchies of switches, connected at the top by one crossover cable to form one fault tolerant network.  Tree A is yellow Tree B is green
Fault tolerance	Fault tolerance is achieved by supplying multiple communication paths between nodes.

For additional definitions of terms and acronyms, refer to the Dictionary.

## 1.2 Fault Tolerant Ethernet (FTE) functional overview

### Related topics

- “Functional Overview” on page 10
- “Communication between FTE nodes” on page 10
- “Fault recovery information” on page 11
- “Using FTE with existing systems” on page 11
- “FTE transmission support” on page 11

### 1.2.1 Functional Overview

Fault Tolerant Ethernet (FTE) is the control network of Experion. It is dedicated to the control mission providing fault tolerance, quick response times, determinism, and the security required for industrial control applications.

FTE is a single network topology with redundancy. This redundancy is achieved using Honeywell’s FTE driver and commercially available components. The driver and the FTE-enabled components allow network communication to occur over an alternate route when the primary route fails. Each FTE node is connected twice to a single LAN through the dual Network Interface Card (NIC) as shown in the following figure.

With R430, ENIM/EHPM are part of the FTE network. For further information, refer to the *Integrated Experion-TPS User's Guide*.

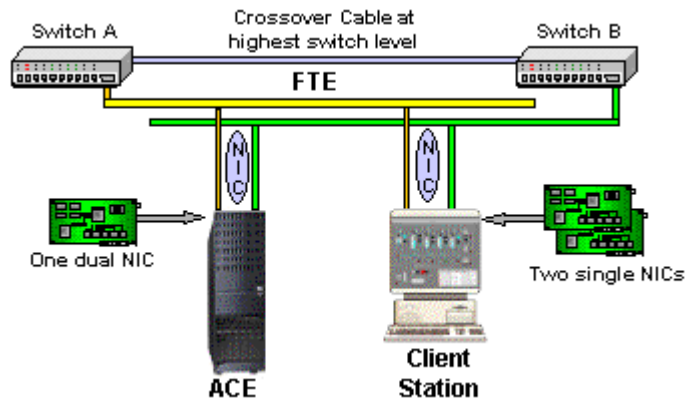


Figure 1: FTE Dual Network Connections

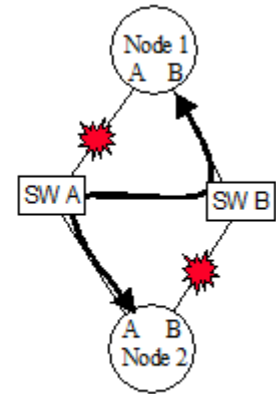
### 1.2.2 Communication between FTE nodes

The following figure and table illustrates how FTE continues to communicate in the event of a failure. Even with a broken channel on FTE Node 1 (Channel A) and FTE Node 2 (Channel B) the nodes continue to communicate from FTE Node 1’s Channel B to FTE Node 2’s Channel A.

Sending Channel	Receiving Channel	Channel Path	Path Status
Channel A	Channel A	1	0
Channel B	Channel B	2	0
Channel B	Channel A	3	1
Channel A	Channel B	4	0

1 == channel is healthy

0 == chanel is broken



### 1.2.3 Fault recovery information

The following table describes the four types of failures from which FTE can recover, and continue to provide communication between nodes.

Type of failure	Description
Complete failure	A network component can neither transmit nor receive data packets.
Partial failure	A network component can either transmit or receive data packets, but not both.
Crossed-cable fault	Cable A is connected to the interface B of a node and cable B is connected to the interface A.
Certain multiple failures	— (N + 1) th failure may occur before the previous N failures are repaired, where N > 0.

### 1.2.4 Using FTE with existing systems

FTE hardware and software components can be installed on existing TPS, PlantScape and Experion systems. Contact Honeywell to determine the compatibility of an existing system.

### 1.2.5 FTE transmission support

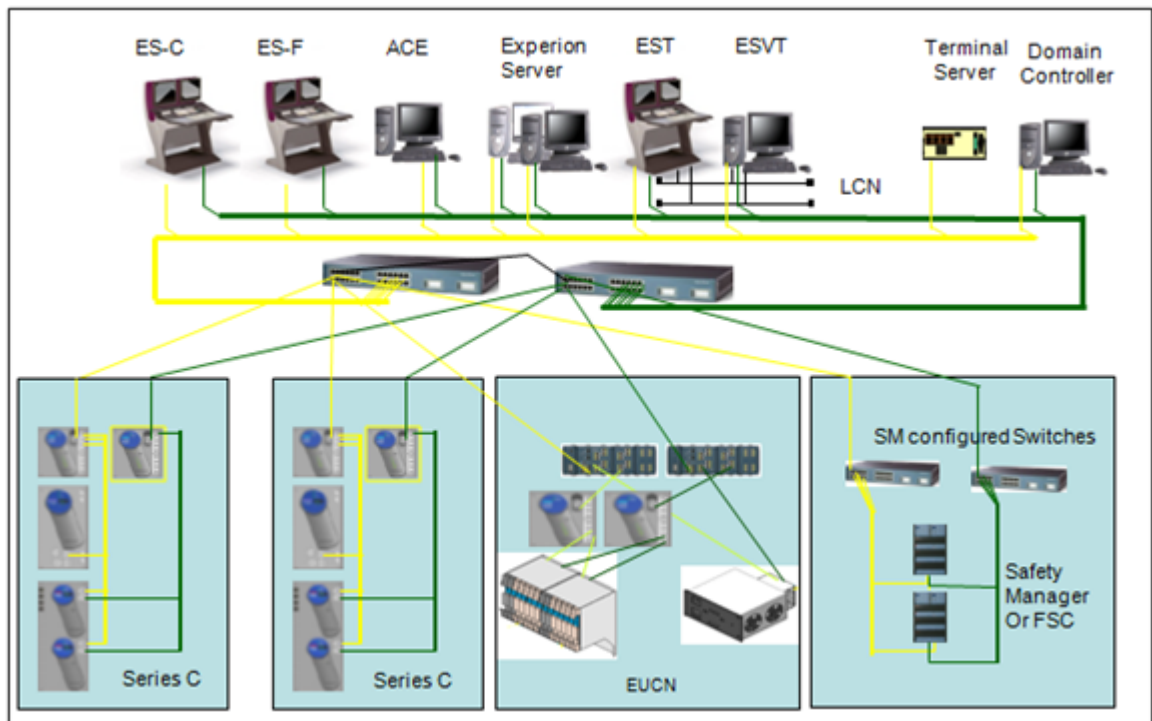
FTE supports the following two types of application traffic.

- Unicast (TCP/IP and UDP/IP).
- Multicast/broadcast (IP Multicast).

## 1.3 FTE network overview

FTE is a single LAN topology with redundancy. An FTE network has two parallel tree hierarchies with redundant switches. The highest level of switches is inter-connected using a crossover cable. The FTE network contains other redundant networking components such as switches, cabling, and redundant network interface adapters. The following figure shows an example of a basic FTE network.

With Experion R430, ENIM/EHPM are part of the FTE network. Refer to the *Integrated Experion-TPS User's Guide* for further information.



### Related topics

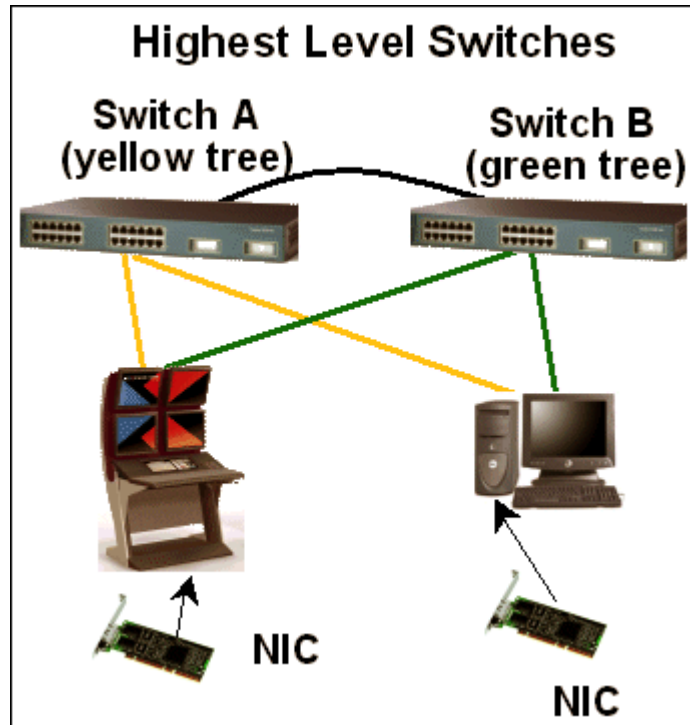
- “FTE community” on page 12
- “FTE tree” on page 13
- “FTE groupings and switch pairs” on page 13
- “FTE nodes” on page 13
- “FTE media components” on page 14

### 1.3.1 FTE community

An FTE community is a group of nodes that have fault tolerant communication coverage using FTE test messages. The FTE community uses a common multicast address for the FTE test messages. These nodes are all members of the same broadcast domain. Nodes that have single connection or dual connection but do not run FTE are also members of the FTE community. Experion systems do not operate properly with multiple FTE communities in the same broadcast domain. Honeywell recommends each FTE community be in a separate broadcast domain.

### 1.3.2 FTE tree

FTE topology is a combination of two parallel tree hierarchies of switches. Each hierarchy can have up to three levels of switches. The switches at the highest level connect to a single FTE network. The two trees are distinguished by color coding and tagging of cables, switches, and FTE node ports. The following figure illustrates an FTE tree.



- Tree A is *yellow*: Each node's network adapter port defined as A is connected to switch A using a yellow color-coded cable. The A ports, yellow cables and A switches form the *Yellow tree*.
- Tree B is *green*: Each node's network adapter port defined as B is connected to switch B using a green color-coded cable. The B ports, green cables, and B switches form the *Green tree*.

### 1.3.3 FTE groupings and switch pairs

Each FTE node has two ports (A and B) that connect to a pair of switches (one for tree A-yellow and one for tree B-green). An FTE grouping is a collection of nodes associated with the same process unit. It is a collection of server(s), stations, and controllers, which usually have high intercommunication. To minimize the number of switches and the wiring between nodes in a grouping, the nodes connect to the same pair of switches. If the plant topology does not support nodes in a grouping to connect to the same pair of switches, nodes can also connect to different pairs of switches, and communication continue to function normally.

### 1.3.4 FTE nodes

FTE nodes are nodes with the necessary redundant media components and Honeywell FTE software. FTE nodes connect to the LAN using redundant network interface adapters (FTE nodes require one unique IP address assigned to the virtual adapter created by the FTE driver). FTE nodes are resilient to single Ethernet failures such as, switch or cable faults, and are able to communicate if at least one path exists between them.

### 1.3.5 FTE media components

Refer to the latest *Fault Tolerant Ethernet (FTE) Specification and Technical Data* for information on the latest qualified components for your FTE network.

## 2 Planning a Honeywell network

### **Related topics**

“Before you begin” on page 16

“FTE network infrastructure” on page 17

“FTE best practices summary” on page 19

---

## 2.1 Before you begin

### Related topics

“Assumptions” on page 16

“Network services consulting and support for FTE” on page 16

“Planning an FTE network” on page 16

### 2.1.1 Assumptions

Users installing and configuring an FTE network must have knowledge on networking concepts and requirements, including design, maintenance, and security. This includes network administrators and control engineers.

### 2.1.2 Network services consulting and support for FTE

The *Global Project Operations Networking Group* provides consulting, design, configuration, and implementation for all aspects of networking on Experion projects. The *Open System Services Group* provides consulting on FTE network architectures and their integration with higher-level networks, including consulting, configuration, and support services for firewalls.

### 2.1.3 Planning an FTE network

Ensure that you consider the following network requirements before you begin installing your FTE network.

- Be familiar with FTE topology, including the maximum number of FTE nodes.
- Plan your FTE network including the placement of major components, cable segment lengths and limits, and cable routing.
- Understand the security and communication requirements for each level or layer within the FTE network.
- Plan the use of firewalls, if necessary.
- Consider your network security requirements.
- Establish subnet or domain for your FTE network.
- Determine all network settings, including the FTE nodes' IP addresses.
- Verify software and media requirements.
- Plan IP address distribution.



## 2.2 FTE network infrastructure

An FTE network comprises of different node types and network devices. This section describes the considerations and requirements for connecting and configuring these devices to provide a system that has significant security and reliability improvements over a simple Ethernet network.

### Related topics

“Plant network levels” on page 17

“FTE community” on page 12

“Maximum nodes within an FTE community” on page 17

“Large FTE systems” on page 17

### 2.2.1 Plant network levels

A plant network has four layers or levels. Level numbers are used to simplify the description of the node location within the network hierarchy.

The FTE network of an Experion system includes the following levels.

- Level 4: Plant level applications.
- Level 3: Advanced control and advance applications (non-critical control applications).
- Level 2: Supervisory Control, Operator HMI (HMI, and Supervisory Controllers).
- Level 1: Real time control (controllers and IO).

### 2.2.2 FTE community

An FTE community is a group of nodes that have fault tolerant communication coverage using FTE test messages. The FTE community uses a common multicast address for the FTE test messages. These nodes are all members of the same broadcast domain. Nodes that have single connection or dual connection but do not run FTE are also members of the FTE community. Experion systems do not operate properly with multiple FTE communities in the same broadcast domain. Honeywell recommends each FTE community be in a separate broadcast domain.

### 2.2.3 Maximum nodes within an FTE community

Each FTE community can have a maximum of **300** FTE nodes and **200** single connected Ethernet nodes. While determining the maximum number of nodes, consider FTE nodes that are visible on the network, but DO NOT share the same FTE multicast address. UDP source port and UDP destination port are considered as two separate single connected Ethernet nodes.

Single or dual connection	Characteristics	Network view
Dual connection node with FTE driver software	Node shares the same FTE multicast address, UDP source port and UDP destination port as the other FTE nodes within the same community.	Considered as a FTE node when it shares the same multicast address. If the node is outside the multicast scope, it is seen as a non-FTE node.
Single connected Ethernet nodes	Node can communicate.	Considered as a non-FTE node.

### 2.2.4 Large FTE systems

The limit for FTE nodes does not restrict large systems from being considered as FTE communities, since FTE communities can be interconnected using a router. Individual FTE communities must be designed to include nodes that have critical intercommunication requirements. Distributed Server Architecture (DSA) can be used to

share data between routed FTE communities. Using this technique, a large system of FTE nodes with a wide geographical distribution can be constructed.

## 2.3 FTE best practices summary

The topology diagrams in this document represent Honeywell's recommended best practices for installing a large system. While variations of the architecture are possible, the topology examples represent the highest level of security and reliability.

The emphasis is on isolating critical areas of function using layers of switches such that the hierarchy is maintained in the following order, starting with the most important.

- Local peer-peer control.
- Peer to external peer.
- Controller to server/station.
- Server to station, ACE and other Level 2 nodes.
- Communication from Level 2 to Level 3.

Communication from Level 2 to Level 3 is generally less critical and more restriction can be placed on this path.

### Related topics

"FTE critical configuration items" on page 19

### 2.3.1 FTE critical configuration items

The following list displays configuration items that are CRITICAL to the reliability and security of the Experion FTE control network.

Requirement	Reference
Level 1 nodes must not have a default route configured.	Section 3
Honeywell Control Firewalls must be connected to switch interfaces configured for portfast.	Section 3
Routers must have the access lists added for proper filtering of traffic to Level 2.	Section 4
Use hot standby protocol (HSRP) if multiple connections to Level 3 are required.	Section 5
A firewall between Level 4 and Level 3 is critical to the security of the control nodes on Level 2 and Level 1.	Section 6
Multiple communities on a single subnet are not recommended.	Section 8
Server IP addresses are in a separate range from other nodes.	Section 8
Use DHCP or BootP for all non-Honeywell nodes.	Section 8
Private IP addresses should be used where possible with NAT to corporate networks.	Section 8
Level 1 addresses must be in a separate, reusable range when communication with Level 4 is necessary.	Section 8
Level 2 nodes that communicate with Level 1 nodes must have an appropriate address range configured.	Section 9
Router at Level 3 device that interfaces to level 2 devices MUST have no IP proxy-arp configured.	Section 9
Switches are configured with the Honeywell configuration files.	Section 9
Experion nodes and switch/router uplinks (downlinks) must be connected to appropriately configured interface ports on the switches.	Section 9



## 3 Level 1 nodes

### **Related topics**

“About level 1 nodes” on page 22

“Level 1 best practices” on page 23

## 3.1 About level 1 nodes

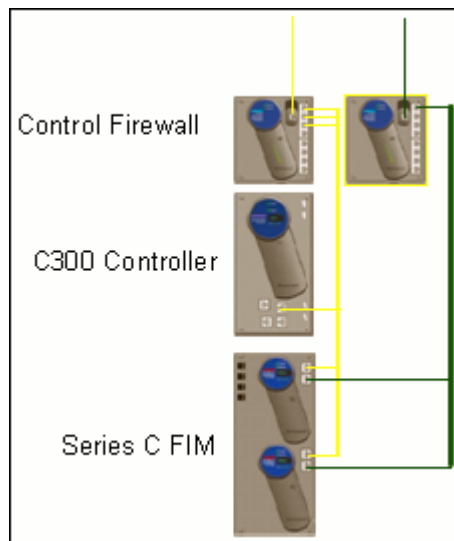
Level 1 nodes are the heart of the control system. This network segment contains the following:

- Controllers
- FTEB-based I/O
- Series A or Series C FIM nodes

### 3.1.1 Series C Level 1 LAN cluster

The following diagram shows a Series C Level 1 LAN cluster, the main purpose is to allow critical peer-to-peer traffic flow only locally.

With Experion R430, ENIM/EHPM are part of the Series C Level 1 LAN cluster. Refer to the *Integrated Experion-TPS User's Guide* for further information.



#### Citizenship

- Controller (C300)
- Series C Fieldbus Interface Module
- Control firewall
- FTEB with 1756 I/O
- ENIM/EHPM

#### Level 1 control firewalls

- Provide point-to-point connectivity.
- Cyber security
- Prioritization of inside packets over outside packets

## 3.2 Level 1 best practices

The best practice for Level 1 nodes is to place them on a separate switch pair or a Honeywell Control Firewall pair. C300 nodes must be connected to Honeywell control firewalls. This allows critical peer-to-peer traffic that cannot tolerate a communication delay longer than 250 ms followed by an FTE cable fault. It also gives controllers a level of isolation from other nodes during catastrophic failure or network disturbance. Arrange the critical elements of control to be connected to the Level 1 switch pair. As this level includes controller nodes, the critical control traffic must have adequate bandwidth. Complying with the best practices in this section ensures you have sufficient bandwidth.

### 3.2.1 Honeywell Control Firewall best practices

Experion R300 introduced the Honeywell Control Firewall, an appliance that protects the Level 1 Series C nodes against unwanted traffic from Level 2 and above nodes. All Series C nodes including C300, Series C FIM, ENIM/EHPM, and FTEB-based 1756 I/O must be connected to the internal interfaces of a Honeywell Control Firewall. Do not attach the uplink of the Honeywell Control Firewall to a Level 1 or Level 2 Cisco switch using an interface configured as an uplink. Configure all Control Firewall interfaces for portfast before attaching the Control Firewall. Otherwise, interfaces connected to Control Firewall gets blocked and causes loss of view upon recovery of a root switch in a network, which causes recalculation of the switch spanning tree topology. Control Firewalls do not use spanning tree. You cannot cascade Control Firewalls – that is one Control Firewall cannot be connected to another.



#### Attention

- PC nodes, including temporary debug laptop, must not be attached inside the Honeywell Control Firewall. The NETBios return messages are blocked and the PC node becomes the master browser. This prevents proper file sharing from occurring on the entire network.
- ICMP messages are blocked. Hence, common debug applications like Ping and Traceroute do not work.

### 3.2.2 Honeywell Control Firewall features

The Honeywell Control Firewall has the following features.

- Allows only CDA connected traffic using TCP port filtering.
- Limits broadcasts to ARP and Bootp and limits the rate.
- Limits the rate of connection to mitigate SYN flood attacks.
- Limits multicast to FTE messages.
- Allows NTP time sync packets, but limits the rate.
- Prioritizes internal packets over external packets.
- No user configuration required.

### 3.2.3 C200 with FTEB best practice

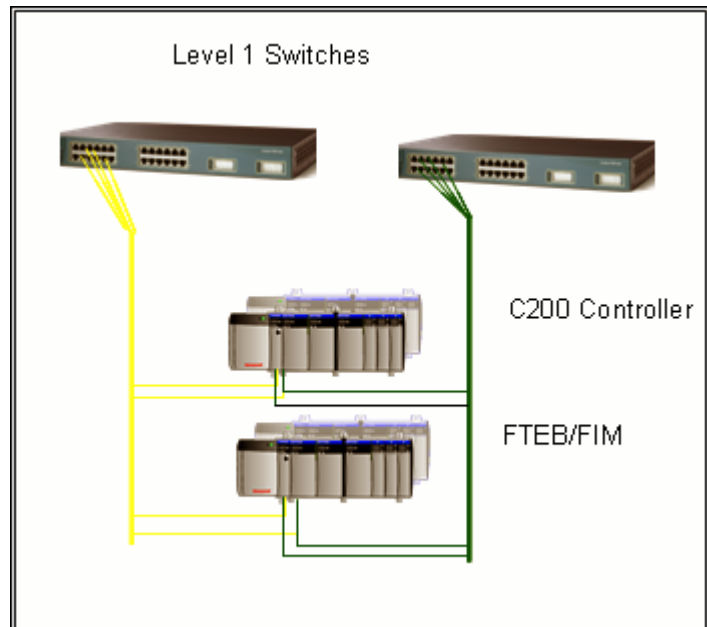
Installations with C200 controllers connected to FTE with the FTEB must be connected to a Cisco switch with a Level 1 configuration installed. Several settings in the Honeywell switch configuration files enable protection for Level 1 traffic. Other best practices include the following:

- TCP ports used for critical control and display traffic are fixed and familiar. When a packet with these TCP port values are received, the Cisco switches are notified that this packet must be given priority.
- The uplink interface on the Cisco Level 1 switch is configured to limit the amount of broadcast and multicast traffic. Broadcast or multicast traffic levels that exceed the limit are stopped. However, other traffic is not affected.
- BPDUguard is configured on non-uplink interfaces to prevent loops and unexpected uplink placement.

The use of an IP subnet for Level 1 nodes outside the subnet range of the Experion servers is not recommended as a best practice. This scheme is recommended for installations where Level 1 address reuse is required. For more information, refer to *Section 8.3, “Reusing IP Addresses for Level 1.”*

### 3.2.4 Series A Level 1 LAN cluster

The following diagram illustrates a Series A Level 1 LAN cluster. The main purpose of this cluster is to allow critical peer-to-peer traffic to flow only locally. With Experion R430, ENIM/EHPM is included in the Level 1 LAN cluster. Refer to the *Integrated Experion-TPS User's Guide* for further information.



#### Citizenship

- Controller (C200)
- Fieldbus Interface Module
- Cisco switches
- ENIM/EHPM
- Safety Manager (SM)

#### Level 1 Switches

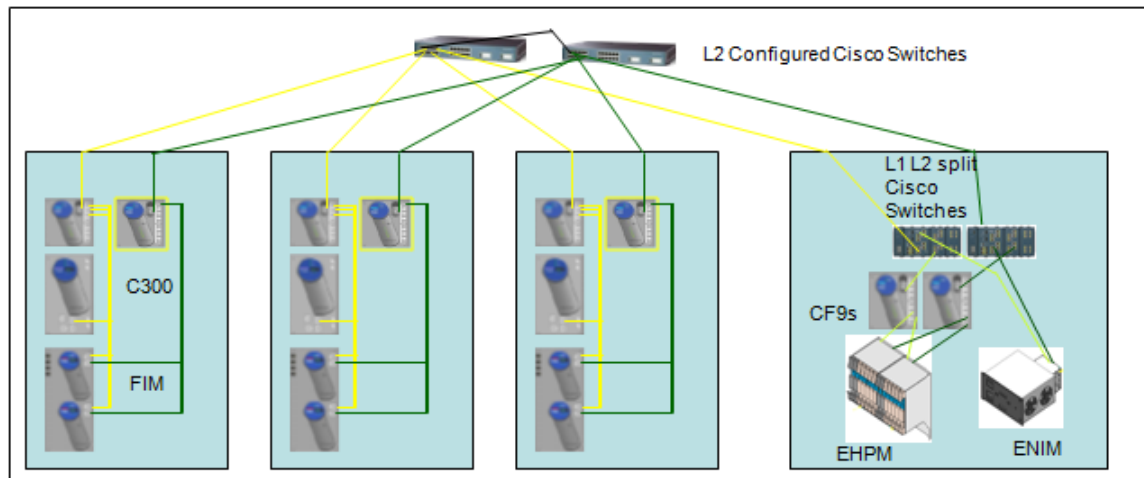
- Provide point-to-point connectivity for FTE devices in the cabinet
- High reliability configuration
  - Always redundant
  - Configure CDA traffic as the highest priority switch queue
  - Configure view traffic as the second highest priority queue
  - Configure other traffic as low priority switch queue

### 3.2.5 Connecting Level 1 LAN clusters

The following diagram shows several Level 1 LAN clusters connected with a second layer of switches.

With Experion R430, ENIM/EHPM is included in the Level 1 LAN cluster. Refer to the *Integrated Experion-TPS User's Guide* for further information.





### Citizenship

- L2 configured Cisco switches
- L1 configured switches
- Level 1 LAN clusters

### Cisco Switches

- Connect Level 1 clusters
- High reliability configuration
  - Configured bandwidth limits for broadcast, multicast storm suppression
  - Ability to disable interfaces with high traffic conditions
  - Automatic port enabling when traffic profile returns to normal
- Dual Cisco switch faults impact *inter-cabinet* traffic only

## 3.2.6 Connecting Level 1 nodes that intercommunicate

The best practice is to connect Level 1 nodes that intercommunicate to the same switch pair, so that they have the shortest communication path. If this is not possible due to size or geographic dispersion, their communications go through the Level 2 switches. The Level 2 switches must be configured with the same quality of service approach as those used for Level 1 switches.

- TCP ports are given the prioritization scheme described for Level 1.
- The control traffic entering from a Level 1 switch is tagged with the highest priority at the ingress.
- The output queue to the destination Level 1 node sends the control traffic before any other traffic.

Communications redundancy is provided for this peer-to-peer traffic by always having two “pipes” from peer-to-peer and using FTE to provide four possible paths. Additionally, Level 2 switches are configured to have storm protection on the interfaces where Windows operating system nodes reside. This storm protection prevents broadcast or multicast storms caused by a node that is infected and using a denial-of-service attack. If a node reaches a limit of 20% of the connection bandwidth being used for broadcast or multicast, the interface is cut off until the traffic level falls below 18%. Normal FTE traffic for broadcast and multicast is below 2% for each. Recent switch configuration files for the latest switch types use explicit bandwidth limiting (defined as Mbps) rather than percentage based limiting. Refer to *FTE Technical and Specification Data* for more information on types of switches supported.

## 3.2.7 Using a switch for level 1 and level 2 (split switch configuration)

It is possible to divide a single switch into a level 1 and a level 2 section. The sections are interconnected by a cable between a port on each so the switch actually has 22 ports instead of 24 ports. The switch still counts as

one level in the network hierarchy. The split configuration reduces the number of switches needed to implement best practices for connecting a few Level 1 and Level 2 devices. If you must put the Level 2 Console station directly on the Level 1 switch, the best practice is to use the split switch configuration files. These files provide improved isolation between Level 1 and Level 2. Refer to section 9.6, “*Honeywell’s Switch Configuration Files*” for information of switch configuration options.

## 4 Level 2 nodes

### **Related topics**

“About level 2 nodes” on page 28

“Level 2 Best Practices” on page 29

“Implementing level 2 best practices” on page 31

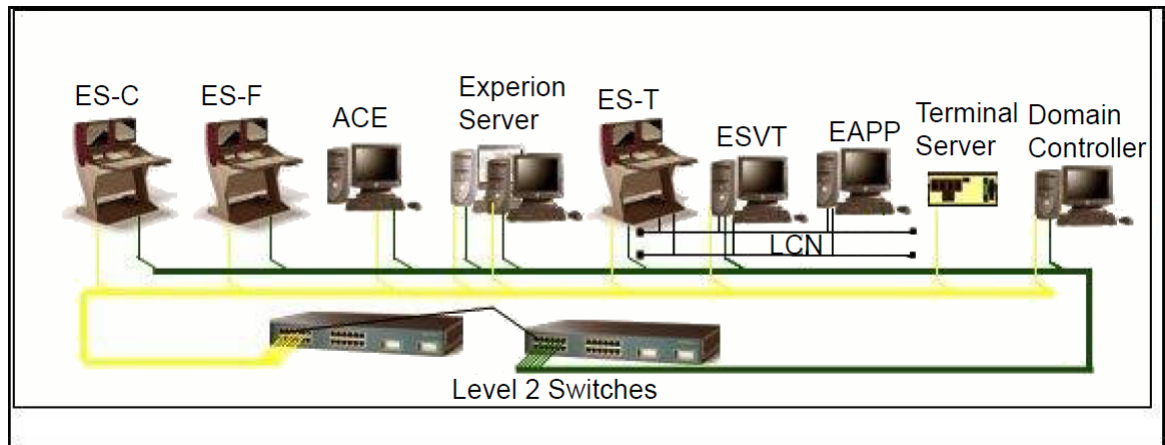
“Safety Controller Best Practices” on page 33

## 4.1 About level 2 nodes

Level 2 nodes are primary server, view and advanced control nodes for the process control system. These nodes are essential for operation of the process, but not as critical to control as the Level 1 nodes. For example, servers, stations, ACE nodes, and PHD nodes.

### 4.1.1 Level 2 LAN

The following diagram illustrates an example of Level 2 LAN.



#### Citizenship

- Experion server
- Experion console
- Application node
- Subsystem interfaces
- Domain controller
- Cisco switches
- Experion App node

#### Level 2 Cisco switches

- Point-to-point connectivity for Level 2 devices
- Pre-configured bandwidth limits for broadcast, multicast storm suppression
  - Ability to disable interfaces with high traffic conditions
  - Automatic port enabling when traffic profile returns to normal
- Configured CDA traffic in high priority switch queue (ACE-ACE, ACE-Controller)
- Configured non-CDA traffic in low priority switch queue

## 4.2 Level 2 Best Practices

The nodes residing on Level 2 are vulnerable to attacks by virus or software glitches because of the open nature of the operating system and the customized software running on these nodes. Hence, the Cisco switches in Level 2 are configured to provide the security and reliability as described in “Connecting Level 1 nodes that intercommunicate” on page 25.

### 4.2.1 Configuring level 2 switch

The following are configured in the Cisco switches.

- Protection from broadcast and multicast storms on all interfaces to these open nodes.
- The display traffic, like the control traffic, has a higher priority so that the view to the process traffic takes precedence over other traffic on the switch. This is important if there is a “bad actor” on the LAN that generates high traffic. The traffic with higher priority control and view arrives first.
- BPDUguard is configured on non-uplink interfaces to prevent loops and unexpected uplink placement.

### 4.2.2 Avoiding multiple network connections

Avoid connecting PC nodes to multiple networks. For example, connecting a server to two networks turns the PC node into a router, which is not allowed. Instead, the Experion network structure provides the use of routers to combine Level 2 nodes to Level 3 nodes or to other Level 2 nodes. A built-for-purpose router must be used to provide security and reliability through the use of access list filtering. There are exceptions when a third NIC interface is used for private connection to a single Ethernet device. An example is the Honeywell DHEB for bridging to the Data Hiway.

### 4.2.3 Non FTE dual attached nodes within level 2

Non-FTE dual attached nodes connect to Level 2 switches and are compatible with FTE. Although these nodes communicate with FTE nodes, they do not have the same level of network availability as FTE. Examples of these node types are as follows:

- Terminal servers
- OPC servers
- PLCs

### 4.2.4 Non FTE single attached nodes within level 2

Non-FTE single attached nodes, such as terminal servers or subsystem devices connect to Level 2 switches. For a large number of single attached nodes, use a separate switch to aggregate these nodes.

Following are guidelines for using a switch for this purpose.

- The switch is counted as a level for spanning tree. Hence, it must not be connected to an FTE switch at the third level.
- The switch must not be connected to any Level 1 switches.
- To avoid loss of data, nodes that have a single connection are divided into two switches, where some of the nodes are connected to the green switch and the others are connected to the yellow switch.

### 4.2.5 Nodes with embedded operating systems

Nodes with embedded operating systems do not have the processing power to handle multicast and broadcast traffic volume generated by FTE test messages and Address Resolution Protocol (ARP) packets. Connect these

nodes to a Level 3 switch, or protect it with “access list filtering” on a separate Level 2 switch. Honeywell recommends the use of a qualified Experion switch for this purpose. Contact Honeywell Network Services for switch configuration.

#### **4.2.6 Critical nodes**

Honeywell recommends critical nodes, such as Safety Manager, to be placed on a separate switch. Refer to Safety Controller Best Practices; in Section 4.3.

#### **4.2.7 Best practices for connecting a crossover cable**

FTE networks require a single crossover cable at the top of the hierarchy. In large systems, Honeywell recommends that a 1 Gbps connection be used. In case of multiple faults, backbone traffic passes through this connection. The highest bandwidth must be available for this traffic.

To determine the capacity of the crossover cable, add the total average bandwidths of all the cluster servers. If the amount is greater than 20 Mbps, Honeywell recommends the use of a 1 Gbps crossover cable.

- Use only one crossover cable per FTE community.
- The cable can be placed between any of the Level 2 yellow and green switches, where the yellow switch is configured with the highest spanning-tree root priority and the green switch is configured with the second highest spanning-tree root priority, and the rules of 3 levels of switches are preserved.
- Do not connect the crossover cable to a Level 1 switch.

## 4.3 Implementing level 2 best practices

### Related topics

- “Separate IP address range” on page 31
- “Using filters in level 3 routers” on page 31
- “Domain controllers in an FTE network” on page 31
- “Connecting level 2 to level 1” on page 32

### 4.3.1 Separate IP address range

To increase reliability and security, Level 2 nodes must be divided into two IP address range. Using two ranges simplifies the use of access lists for filtering as described below.

- Servers on Level 2 nodes require access to nodes on other subnets, and a few nodes on Level 3, 3.5/ demilitarized zone (DMZ). Communication to other nodes includes Distributed Server Access (DSA), and engineering access to load control schemes and high-level control.
- Windows Server 2003 (using the R3xx FTE driver) and Windows Server 2008 (using the R400 MUX FTE driver) domain controllers are qualified to run the FTE driver. For a higher level of security, Honeywell recommends a peer domain controller on Level 2. The domain controller must be addressed in the server range if complete communications with a root domain controller on Level 3 is needed.
- Nodes on level 2 must not be accessed by nodes on level 3 and the nodes must be protected from such access.

### 4.3.2 Using filters in level 3 routers

Filtering is used to control node access either the router, or the switch interface that connects to the router. Filtering, which is implemented by creating specific access lists for the Cisco equipment, must accomplish the following:

- Allow servers to have complete two-way communication with other nodes on all levels of the network.
- Allow nodes other than the server, to communicate with domain controllers for authentication and name service.
- Allow level 2 nodes to initiate communication with level 3 domain controllers.

### 4.3.3 Domain controllers in an FTE network

Windows 2003 domain controllers must run R3xx drivers (these are compatible with R400 nodes if they are configured with a matching FTE multicast address and UDP destination port) and Windows 2008 domain controllers must run FTE Mux drivers. For a higher level of security, Honeywell recommends a peer domain controller on level 2. The domain controller must be addressed in the server range if complete communication with a root domain controller is needed on level 3.

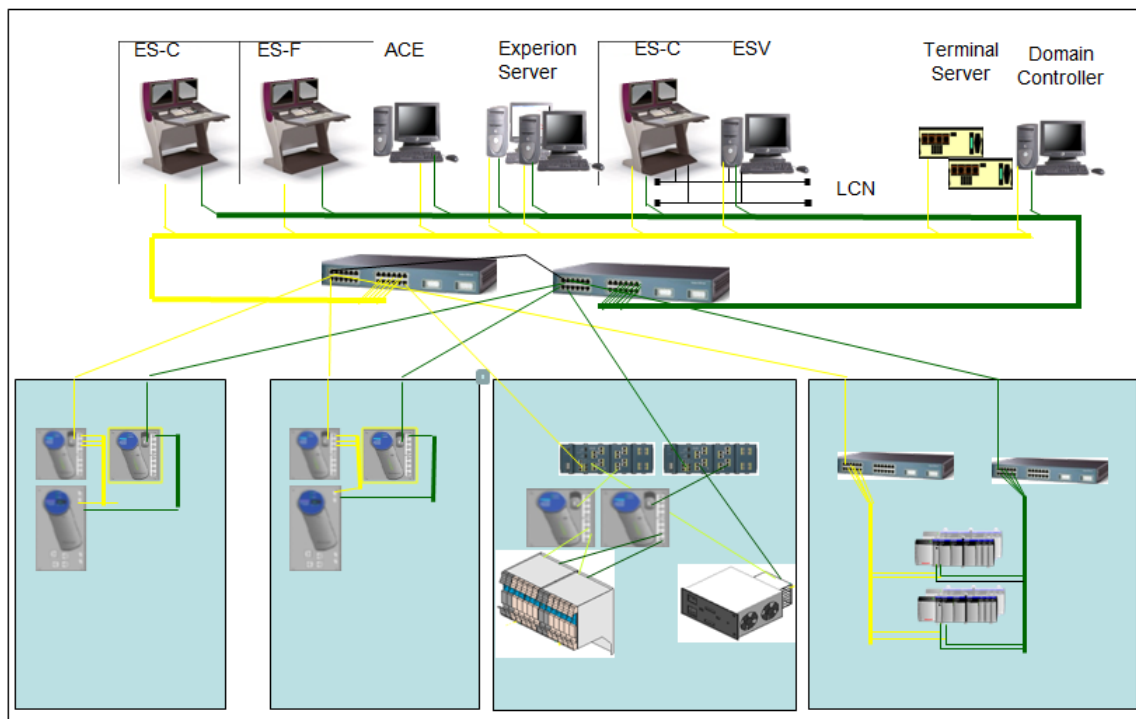
For communities that do not require a higher level of security, or when the local domain controller is offline, provide communication between level 2 nodes and level 3 domain controllers. Add access lists that enable established communications to return TCP packets from level 3 nodes to the beginning of level 2 nodes.

In either case, the established communication is required for passing packets for Kerberos and LDAP. The filter must allow specific UDP port numbers used for these packets. See Section 11.2 for examples of access lists used for filtering.

### 4.3.4 Connecting level 2 to level 1

The following diagram illustrates the level 1 LAN connected to the level 2 LAN with a pair of switches between the two layers.

With Experion R430, ENIM is present in level 1 cluster. Refer to the *Integrated Experion-TPS User's Guide* for further information.



#### Level 1 control firewall

- Blocks traffic not needed for control.
- Higher level of protection for peer-to-peer nodes on same control firewall.
- Prioritizes internal traffic over external traffic.

#### Level 1 Cisco switches

- Prioritizes ingress traffic, non-CDA in low priority queue.
- Ensures level 2 to level 1 supervisory traffic does not disrupt level 1 control.

#### Level 2 Cisco switches

- Provides level 1 to level 2 connectivity.
- Broadcasts, multicasts storm suppression.
- Configures CDA traffic in high priority switch queue (ACE-ACE, ACE-Cx, ACE-FIM, Server-Cx, Server-FIM).
- Configures non-CDA traffic in low priority switch queue.

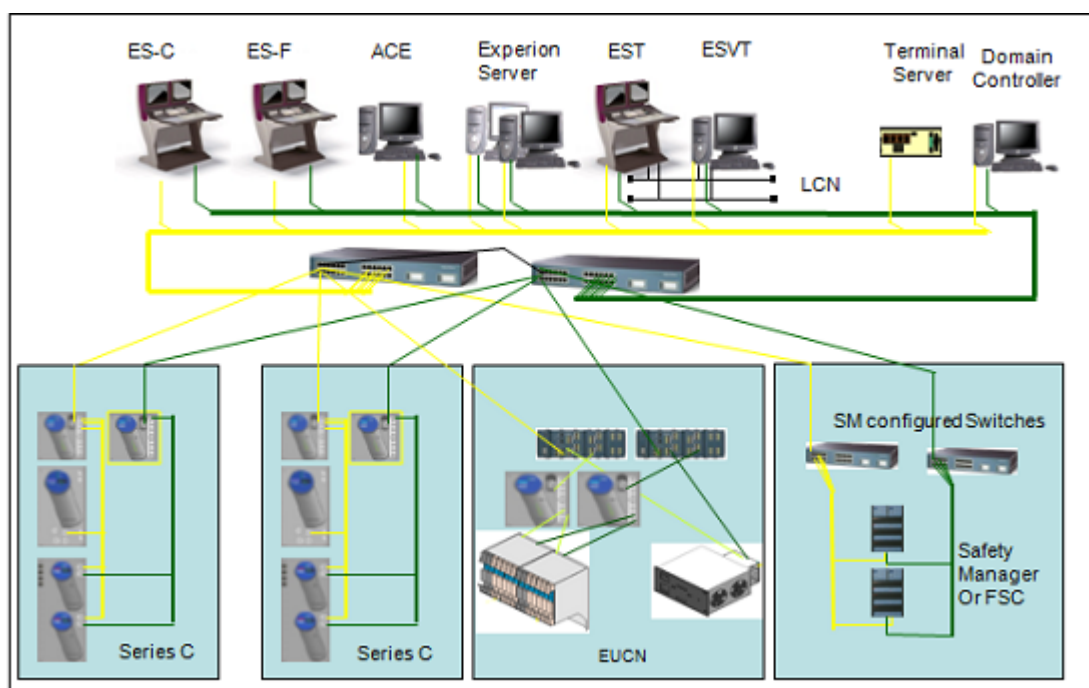


## 4.4 Safety Controller Best Practices

Safety controllers such as the Honeywell Safety Manager, FSC and other third party safety controllers are a special class of nodes that require different implementations depending on their usage in a system. The following sections contain recommendations based on the safety controller's role in the system.

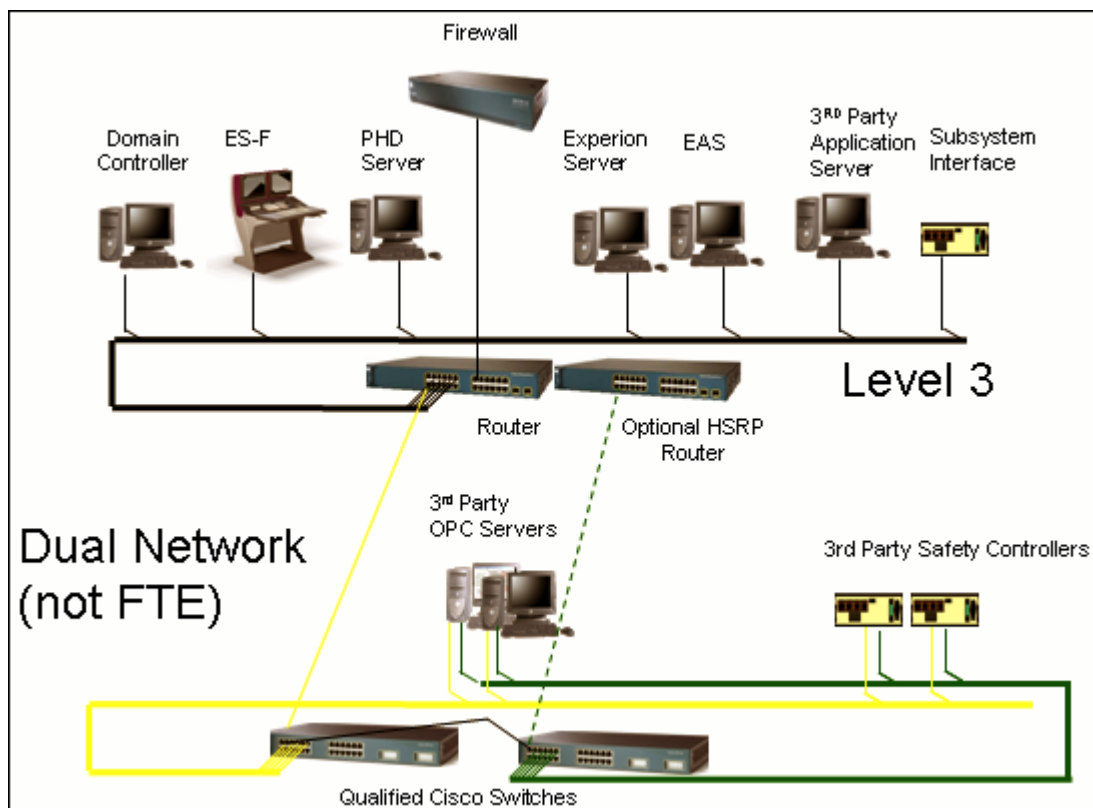
### 4.4.1 Systems with peer-to-peer control communication

For systems that have peer-to-peer control communication with the process-connected controllers such as C200 or C300, the safety controller must be connected to the same FTE community as their peer controllers. These nodes are critical and, Honeywell recommends they be protected in the same way as level 1 nodes, by using a separate switch. This is specifically applicable if you are using FSC. Refer to **Priority Notice PN 2007-07E** on the Honeywell Support website before proceeding further. The switch configuration must be the same as that for level 1 switch used for systems with FTE-based controllers or I/O. Systems with C300s need configurations specific to the controller. Honeywell Network Services provide support for these configurations.



### 4.4.2 Systems using SCADA data only

For systems in which SCADA data only is used, Honeywell recommends that the safety controller be placed in a separate subnet routed to the FTE community where the Experion servers are located. This configuration protects the safety controller and server from unusual broadcast and multicast traffic, without the need for special switch configuration.



## 5 Level 3 nodes

### **Related topics**

“About level 3 nodes” on page 36

“Level 3 best practices” on page 37

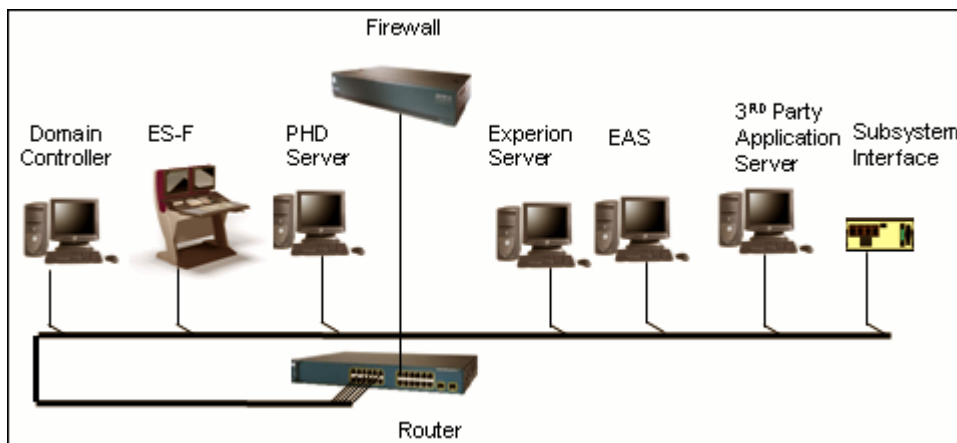
“Level 2 to level 3 best practices” on page 38

## 5.1 About level 3 nodes

In Level 3, all the subnets on the plantwide network, including FTE communities, are tied together. Additionally, the level 3 router is connected to level 4 router through a firewall.

### 5.1.1 Level 3 LAN

The following diagram illustrates an example of a level 3 LAN.



#### Citizenship

- Plant historians
- Applications
- Advanced control
- Advanced alarming
- Router/switch
- Secure gateway to level 4
- Domain controllers
- Subsystem devices
- DSA connected Experion servers
- Stations (monitoring)
- Engineering stations

## 5.2 Level 3 best practices

To accomplish control strategies from one FTE subnet to another FTE subnet, complete access between servers on each subnet must be allowed.

### 5.2.1 Implementing Level 3 best practices

The following list summarizes the networking configuration requirements for level 3 of the FTE network.

- Provide access between FTE community subnets, by grouping servers into an IP address range that can be separated from other level 2 nodes using a subnet mask, as discussed in Section 8.
- Provide a routed interface into level 3. Use of VLANs on the level 3/level 2 interface can cause spanning tree issues and is hence not allowed. However, DO NOT configure IP Proxy-ARP on the routed interface. Note that, this is often enabled by default and you must explicitly disable it.
- The use of unicast for *DSA keepalive* messages is the recommended best practice.
- If you must use multicast, which is not recommended, enable IP multicast routing for the DSA multicast address of 225.7.4.103, and create an access-list filter to allow only this multicast address to pass to the FTE subnets. **Redirection Manager** can use multicast addresses as described in the “Using Redirection Manager (RDM) with Level 3” on page 49.
- Configure each FTE subnet to be in a separate VLAN, which protects the FTE community from unintended access by other nodes on the router.
- Connect only switch A (yellow tree) to the router. If multiple connections to level 3 are needed, refer to “Best practice for multiple connections from level 2 to level 3” on page 49.
- Configure access list filters for the FTE communities that have the following:
  - Allow complete access only to the server IP range.
  - Allow established access to the remainder of the FTE subnet.
  - Deny all other access to the FTE subnet.
- If SFP/GBIC connections are not used, configure the FTE switch’s router interfaces for 100-megabit full duplex.



#### Attention

The router must be connected to a switch interface configured as an uplink port, or to a SFP/GBIC based interface.

- Place each FTE community in a separate subnet. If the level 2 interconnecting device (level 3 switch/router) is a level 3 switch that uses routing functionality, separate VLANs must be configured for each subnet.

### 5.2.2 Using Redirection Manager (RDM) with Level 3

Honeywell’s Redirection Manager can use the FTE multicast test message multicast from the servers to keep track of when the primary OPC server goes off line. Honeywell recommends to only use the multicast when the OPC client is in the same FTE community as the servers. When the OPC client resides in level 3, or when the client is in another FTE community, a mechanism using ICMP must be selected. In this case, ICMP must be allowed between level 3 nodes and subnets.

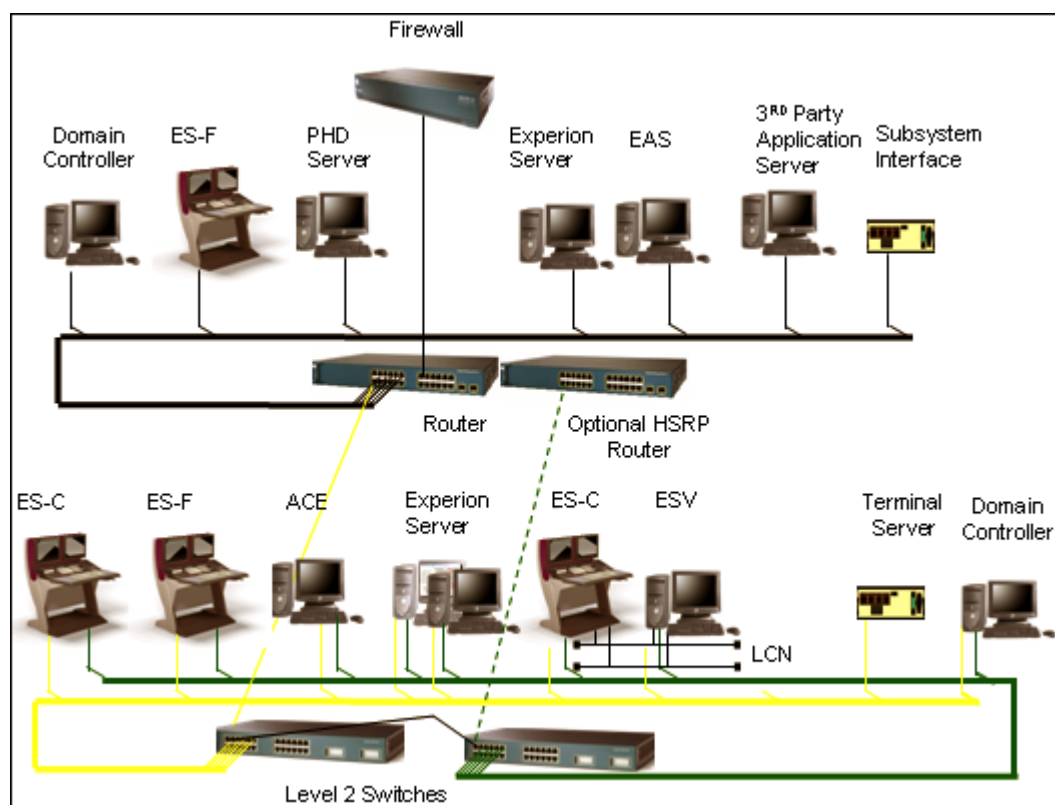
## 5.3 Level 2 to level 3 best practices

### 5.3.1 Best practice for multiple connections from level 2 to level 3

If you require dual connections between FTE backbone switches and level 3, the best practice is to use two routers running the Hot Standby Router Protocol (HSRP). HSRP provides a redundant level of protection in both connection and equipment for the level 3 router. The level 3 nodes can connect redundantly to both routers using dual Ethernet, FTE or they can be single attached to the primary router. The HSRP algorithm protects against level 2 cable failures when the level 3 nodes are single attached. Standardized configuration files cannot be used to configure the router. Honeywell recommends to consult the Honeywell Network Services for router configuration.

### 5.3.2 Connecting level 2 to level 3

The following diagram illustrates the level 2 LAN connected to the level 3 LAN with a router connecting the two layers.

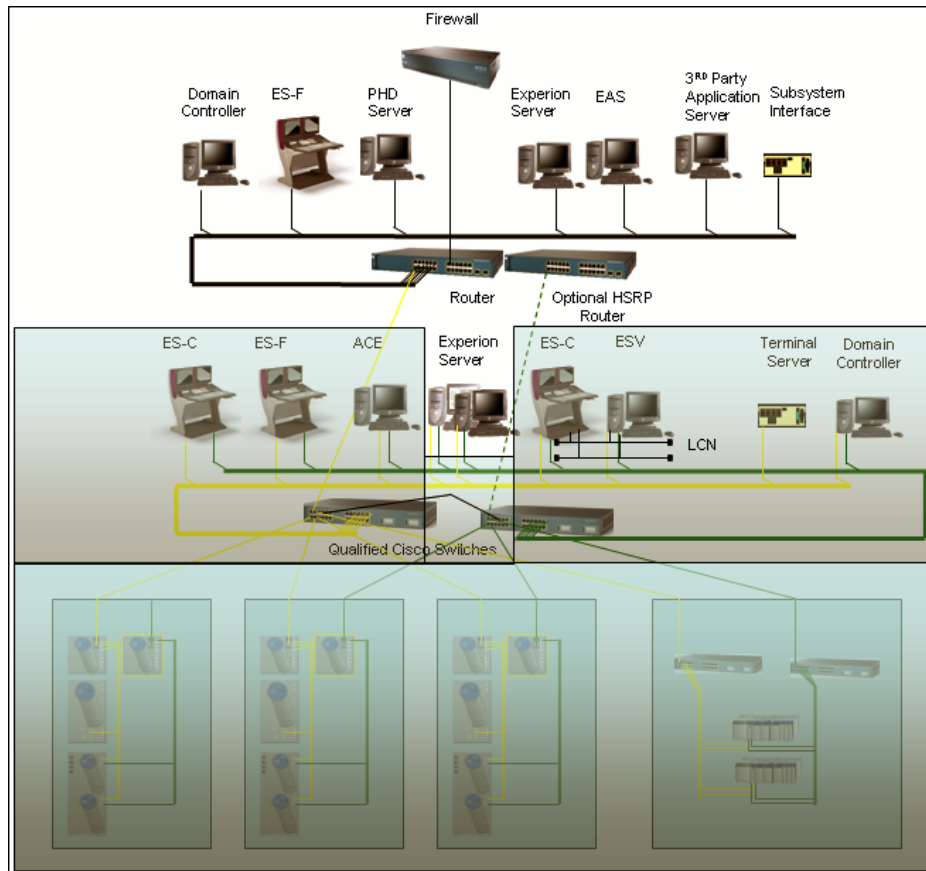


#### Routers and filter

- Cisco 3560 or 3750 – Example router between Level 3 and Level 2.
- Security filter configured to permit communications to and from specific nodes (implemented in Cisco PIX or ASA Firewall).

### 5.3.3 View of level 2 from level 3 with router and filter

The following diagram illustrates level 3's view of level 2 LAN when a router and filter are used. Nodes that are not visible are shaded (gray). Note that only the Experion servers are visible to level 3 as these are the only nodes allowed in the filter. The level 1 nodes are not visible to the level 3 nodes.



#### Level 3 router/switch (Cisco 3560, 3750 or equivalent)

- Provides connectivity for level 3 devices and level 2 networks.
- Has customer-defined route between level 3 and level 2.
  - Routes between enterprise IP's on level 3 to private level 2.
- Implements access list filtering
  - Domain controller/management (level 3 domain controllers and level 2 nodes requiring authentication)





## 6 Level 4 nodes

### **Related topics**

“About level 4 nodes” on page 42

“Level 4 best practices” on page 43

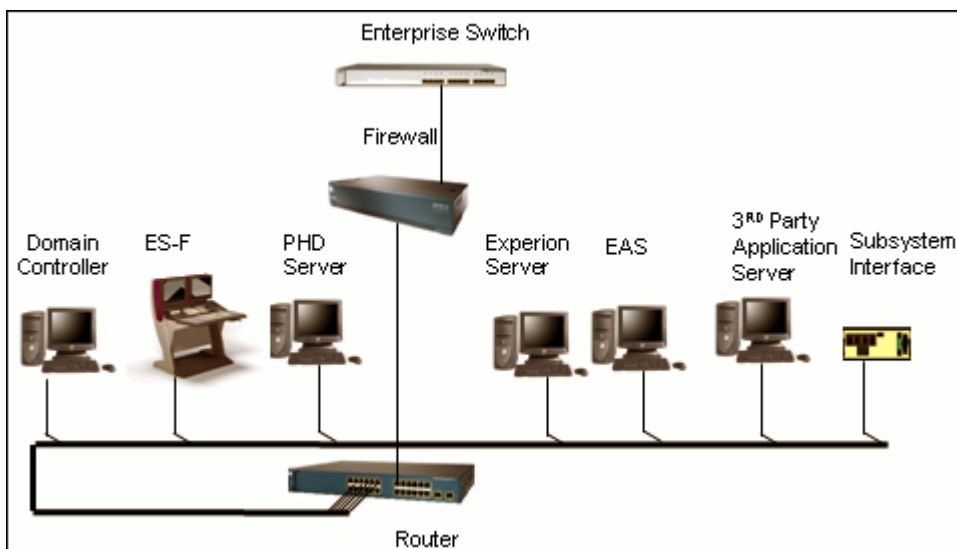
“Implementing Level 4 Best Practices” on page 44

## 6.1 About level 4 nodes

Level 4 is not a part of the control network and the communication on this level is not as secure as that on level 1, level 2 or level 3.

### 6.1.1 Process control network to business network

The following diagram illustrates the connection of the process control network (PCN) to the level 4 (business network) through a firewall and router.



---

## 6.2 Level 4 best practices

As level 4 has a different security and networking environment, Honeywell strongly recommends that level 3 and level 4 be separated by a firewall. Not allowing data to go into more than one network level is a general best practice, and it is important that level 3/level 2 be protected from level 4. Hence, Honeywell recommends a demilitarized zone (DMZ). See “Establishing a DMZ” on page 55.

---

## 6.3 Implementing Level 4 Best Practices

### 6.3.1 Firewall requirements

Firewall requirements between level 4 and level 1, 2 and 3 are as follows:

- If there is a need to use DSA or any other form of communication with level 2 that requires Microsoft RPC or DCOM APIs, the firewall must not use Network Address Translation. See Section 8, “Use of IP Addresses in an FTE Network.”
- The firewall should limit communication to only those nodes on level 4 that require access to nodes on level 3/level 2. However, direct communication between level 4 and level 3/level 2 is not recommended.
- Level 1 nodes must not be allowed to communicate with nodes on level 3/level 4.
- Level 1 nodes must communicate with level 2 nodes on the same subnet only.

### 6.3.2 Router configuration

The router-to-firewall connection must be a single point of connectivity enabling higher security and improved management. An advantage of this is the ability to pull a single cable to create an “air gap” between level 3 and level 4. The connection to the firewall isolates enterprise LAN broadcast and multicast traffic while enabling connectivity between the PCN and enterprise LAN.

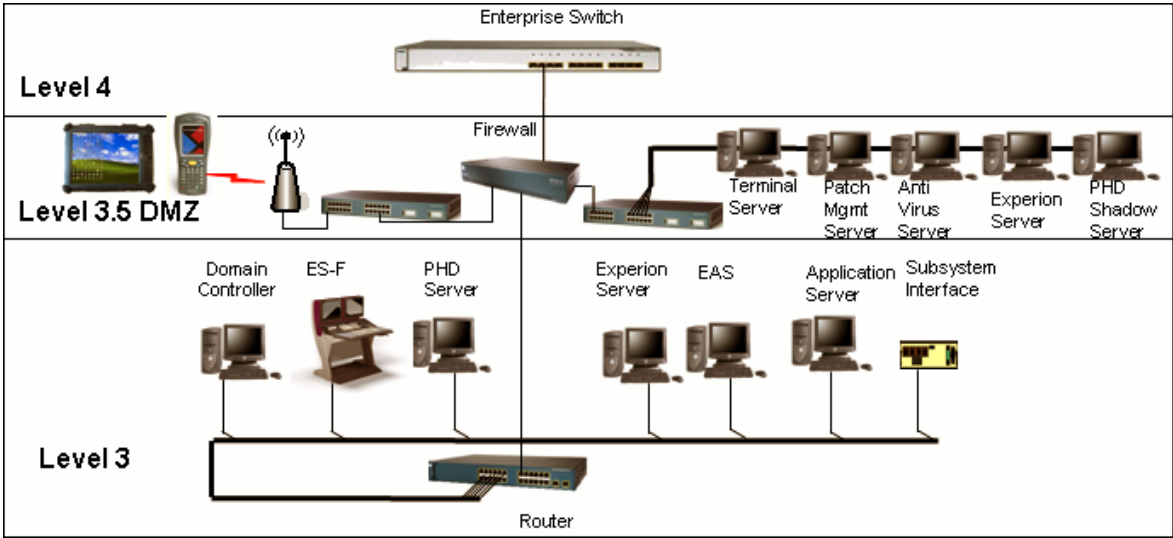
### 6.3.3 Firewall requirements

Firewall requirements between level 4 and level 1, 2 and 3 are as follows:

- If there is a need to use DSA or any other form of communication with level 2 that requires Microsoft RPC or DCOM APIs, the firewall must not use Network Address Translation. See Section 8, “Use of IP Addresses in an FTE Network.”
- The firewall should limit communication to only those nodes on level 4 that require access to nodes on level 3/level 2. However, direct communication between level 4 and level 3/level 2 is not recommended.
- Level 1 nodes must not be allowed to communicate with nodes on level 3/level 4.
- Level 1 nodes must communicate with level 2 nodes on the same subnet only.

### 6.3.4 Establishing a DMZ

If level 4 nodes must access data on level 3, Honeywell recommends you establish a demilitarized zone (DMZ) or a level 3.5 on which only those nodes on level 3.5 can access those on level 4. If required, nodes from level 3 and level 2 can access nodes on level 3.5. Data for enterprise servers can be obtained by having an Experion server in Level 3.5 with DSA access up to level 4 and down to level 3. In addition, terminal servers and virus update file servers can be placed in the DMZ. The DMZ can either be a third leg on the firewall or a separate network between level 4 and level 2 with a firewall between both level 3.5 , level 4 and level 3.5, level 3. For information on establishing a DMZ, see the *Network Security* section in the *Honeywell Network and Security Planning Guide*.



6.3.5 Recommended communication restrictions

The following diagram illustrates the recommended communication restrictions for a level 3.5 DMZ.

	Process Control	Supervisory Control	Advanced Control	DMZ	Business Network
Level	1	2	3	3.5	4
1	NRC	LC	NC	NC	NC
2		NRC	LC	VLC	NC
3			NRC	VLC	NC
3.5					VLC
4					NRC
<b>Legend</b>					
NRC	Not restricted communication				
LC	Limited communication				
VLC	Very limited communication				
NC	No communication				



# 7 Additional Best Practices

## **Related topics**

“Robust FTEB-based topology” on page 48

“Variations on Best Practice” on page 49

“Digital video manager best practices” on page 52

“TPS upgrade best practices” on page 53

---

## 7.1 Robust FTEB-based topology

### 7.1.1 Configuration rules for a robust topology

For critical peer-peer communications that cannot tolerate a communication delay longer than 250 milliseconds following an FTE cable fault, the C200s and/or FTE connected FIMs must reside on the same switch pair. Starting from R200, Experion supports three standard Cisco 2950 Switch configuration options.

Experion R300 introduced the Honeywell Control Firewall, an appliance that protects the level 1 Series C nodes against unwanted traffic from level 2 and above. All Series C nodes including C300, Series C FIM and FTEB-based 1756 I/O must be connected to the internal interfaces of a Honeywell Control Firewall.

These configurations along with the guidelines in this section must be followed while configuring FTE topologies for critical and non-critical processes using FTEBs and hierarchical switch configurations.

### 7.1.2 FTEB switch connection guidelines for critical process

For critical processes, the FTEBs must be connected to one or more switches apart from switches used for level 2 nodes. Peer-to-peer recovery times must be considered. These switches must be configured with the level 1 configuration script.

For critical processes, the level 2 nodes must be configured on switches apart from switches used for FTEB modules. These switches must be configured with the level 2 configuration script.

### 7.1.3 FTEB switch connection guidelines for non-critical processes

For non-critical processes, the level 2 nodes and level 1 nodes can be connected to the same switch pair as described in Section 4. You must integrate the split switch configurations provided by the 2960, 3560 or ie3000 series switches.

### 7.1.4 OneWireless best practices

For information on OneWireless best practices, refer to OneWireless Best Practices document.

### 7.1.5 PCDI best practices

For information on PCDI best practices, refer to *FTE Best Practices* document.



## 7.2 Variations on Best Practice

## Related topics

“Remote locations” on page 49

“System with station on split switches” on page 49

“Split switch configuration” on page 50

“Small Experion systems with FTE” on page 50

“Third-party safety equipment” on page 51

### 7.2.1 Remote locations

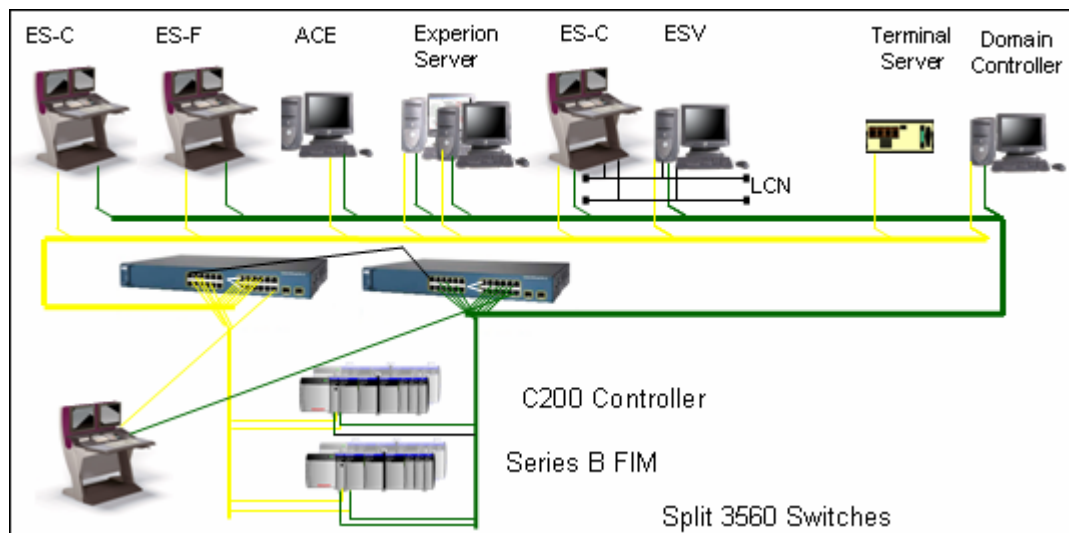
Due to geographic limitations, you may need to modify Honeywell's best practice architecture. For example, you may need to add a level 2 Console station node at a satellite control area to allow a roving operator to view the process, or to allow view of the process in case of a catastrophic break in the communications paths to the control room.

### 7.2.2 System with station on split switches

In some instances, it is allowed to place the level 2 station directly on the level 1 switches. If it is necessary to have multiple level 2 nodes at the remote location, Honeywell recommends that separate switches be used for the level 1 controllers with uplinks to the level 2 switches where the servers and stations reside. The flow of data should be as follows:

- From level 1 switches to local level 2 switches
- To the top-level switch pair at the central location

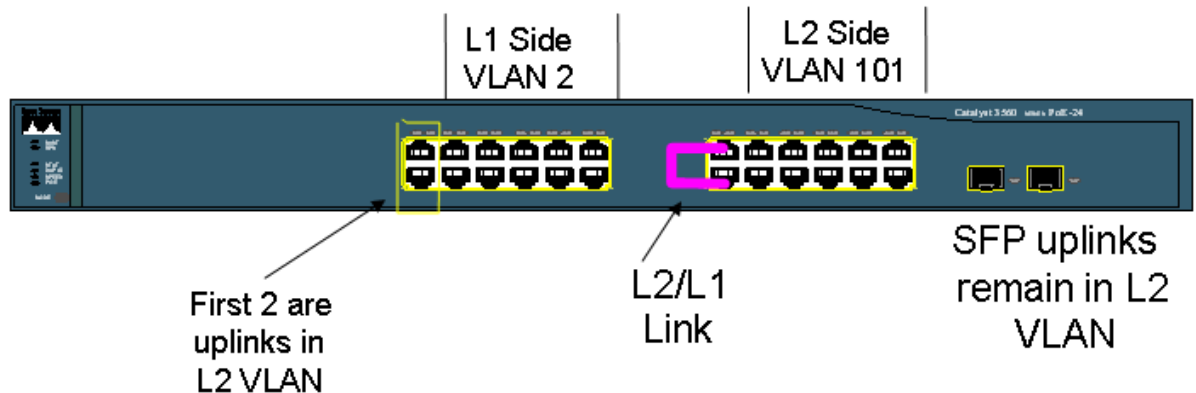
To provide the equivalent of a pair of level 1 switches and a pair of level 2 switches using just one switch pair, Honeywell provides a level 1/level 2 split switch configuration using Cisco 3560, 2960 and IE3000. This switch configuration, is secure than the “mixed” switch configuration, and is recommended to be used.



### 7.2.3 Split switch configuration

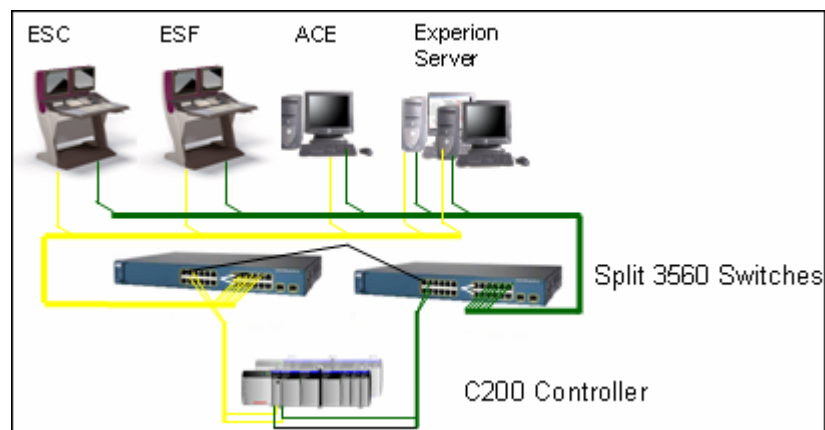
In a split switch configuration, the switch is split in two sections: one for level 2 and one for level 1. The following figure illustrates an example of a split switch with the following characteristics.

- Switch has 10 100T level 1 ports and 10 100T level 2 ports, plus 2 100T uplink ports and 2 SFP uplink ports.
- A new VLAN is created for the level 1 side. Level 2 uses the FTE community VLAN.
- A cross-level cable connects the two VLANs and level 2 to level 1. It must be a crossed cable.
- Spanning tree is configured to prevent blocking between sides.
- BPDUguard is configured on non-uplink interfaces to prevent loops or improper placement of the level1/level2 crossover cable.
- Filtering on the input to the level 1 side passes all CDA TCP ports and all established traffic, all UDP and NTP.
- Multicast policing at 2 Mbps and broadcast storm limits at 1 Mbps are configured.



### 7.2.4 Small Experion systems with FTE

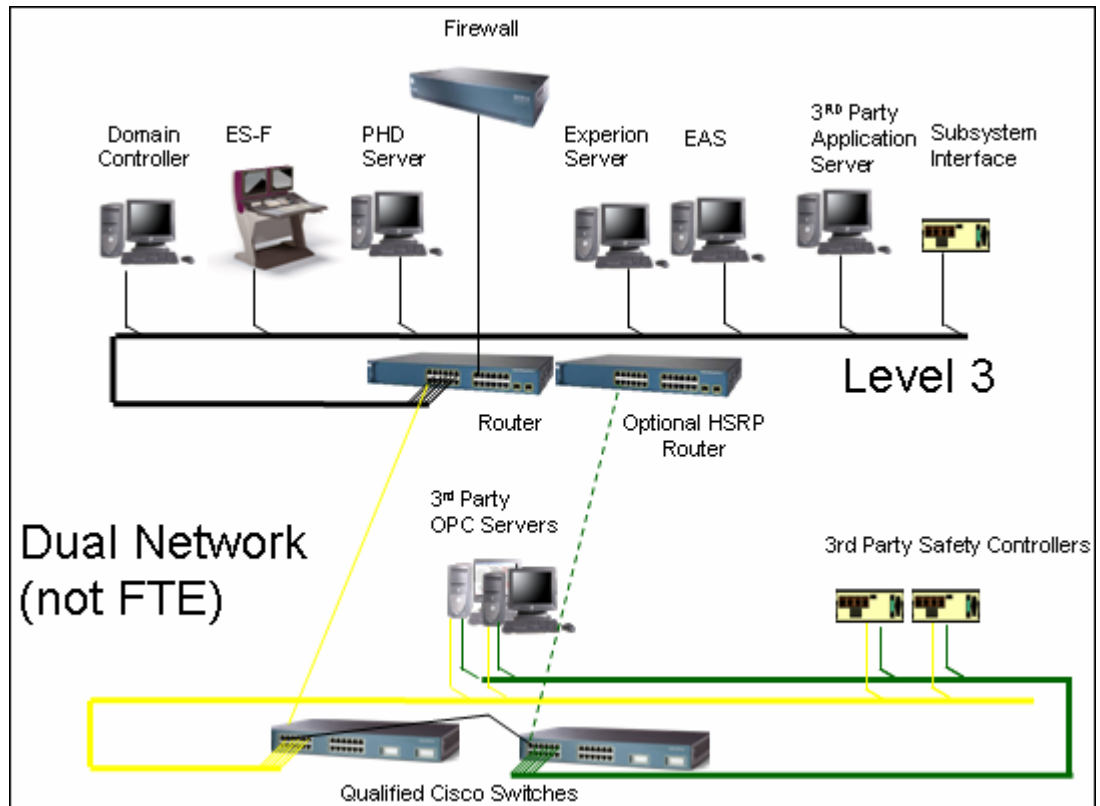
The Experion system is expandable from small systems with only a few nodes to large multi-cluster and multi-FTE community installations. For small systems where all the FTE units are co-located, the best practice topology can be less restrictive to save cost. In this case, all units can be on the same switches. The level 1/level 2 split switch configuration file is used for this installation. Once the installation requires multiple layers of switches or is spread geographically, the Honeywell best practice must be followed.



### 7.2.5 Third-party safety equipment

Third-party safety equipment must be connected directly to the level 2 community for peer-to-peer control applications. Honeywell recommends a split switch configuration to provide level 1 type protection for the safety controller and to provide a level 2 switch configuration for the OPC server.

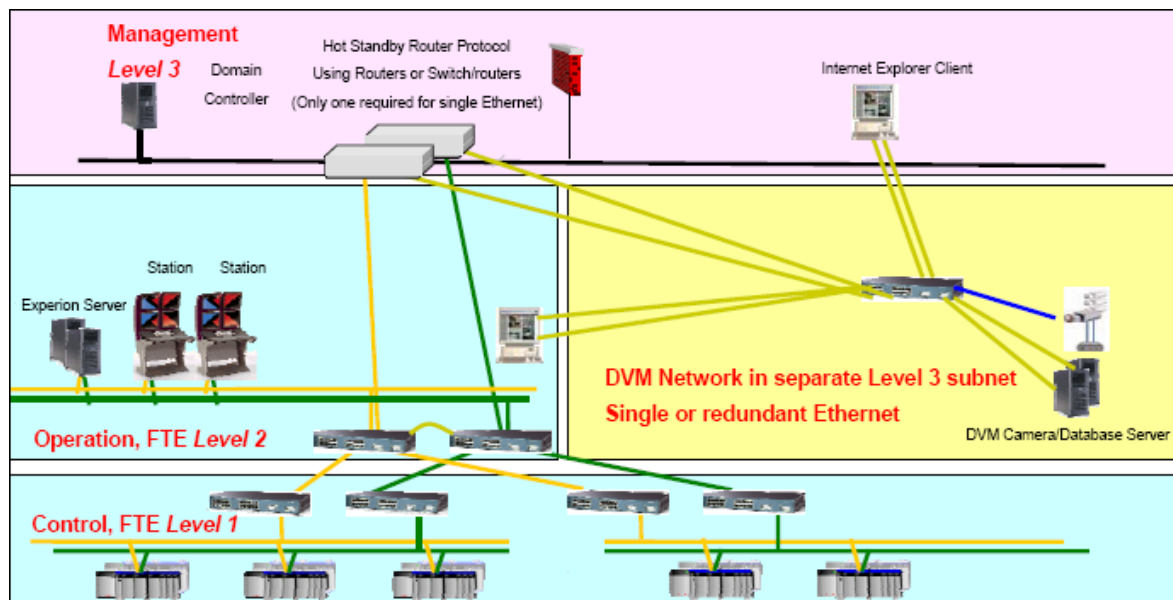
The entry to the controller side of the switch requires special programming to prevent excess broadcast and multicast traffic from entering the switch. Honeywell recommends that the access list on this interface be limited to traffic only from the OPC servers. Honeywell Network Services can provide support for special switch configurations. Section 11.2 contains example access lists.



## 7.3 Digital video manager best practices

The Digital Video Manager (DVM) is capable of consuming a huge amount of bandwidth, depending on the configuration. Hence, Honeywell recommends the following best practices for DVM.

- Create a separate level 3 subnet for the cameras and DVM server.
- Utilize separate display nodes in this subnet for heavy traffic DVM displays.
- Limit the traffic in ES-C, ES-F, and server nodes to less than 20% of the bandwidth.
- Baseline CPU utilization for required DVM displays.
- Always use unicast for DVM. Multicast trips storm limits in the Cisco switches.



---

## 7.4 TPS upgrade best practices

Existing TPS systems can be upgraded with Experion capabilities.

### 7.4.1 Connecting TPS nodes to the FTE network

TPS nodes that are currently connected to an Ethernet Plant Control Network (PCN) can be connected to the FTE network in one of three ways.

- The PCN is a standalone network. It has only control mission nodes connected to the switch(es). In this case, the top of the PCN network can be connected to the top of the FTE switch tree. The *yellow* switch is recommended.
- The PCN is a part of a plant wide network. In this case, the FTE network must be connected to the level 3 network through the existing router with the required filtering described in this document on the interface that connects to the FTE network. If the plant wide network is a single network (without a router), or the existing router does not have the required filtering capability, the FTE network must connect to level 3 through a firewall with the same filtering.
- In case of conversion of the PCN to FTE, the qualified FTE switches must replace existing PCN switches, and FTE software and dual the NIC interface hardware must be added to the TPS nodes.



## 8 Use of IP Addresses in an FTE Network

### **Related topics**

“Introduction” on page 56

“Recommendations for FTE Network Communities” on page 59

“Reusing IP Addresses for Level 1” on page 62

## 8.1 Introduction

With the presence of controller nodes in the FTE community, ensure that you give preference to reliability and security of the network communication. Maximum security is achieved by providing complete isolation in the form of an “air gap” between the control LAN and other plant users. However, this not feasible, as installations require some communication between the control LAN and the plant LAN. Proper IP address management can provide the required security when the control LAN cannot be completely disconnected from the plant LAN.

### Related topics

- “IP address ranges for FTE communities” on page 56
- “IP address range selection recommendations” on page 56
- “IP addresses for non-Honeywell nodes” on page 57
- “Duplicate IP addresses” on page 57
- “Best practices for preventing duplicate IP addresses” on page 57
- “Recovering from a communication loss due to a duplicate IP address” on page 57

### 8.1.1 IP address ranges for FTE communities

Honeywell has developed several recommendations for IP address range selection to increase the security while connecting the control LAN to outside communication networks. In addition to increased security, these recommendations serve to simplify the selection of IP addresses for FTE networks. All examples in this document use an IP address range of 10.n.n.n. Recommendations for IP address range selection are provided for the following types of FTE network communities.

- Isolated FTE community <give links>
- Multiple FTE communities isolated from Level 4 networks
- FTE Communities connected to Level 4 with NO COM communications
- FTE communities connected to Level 4 with COM communications to level 3/level 4

### 8.1.2 IP address range selection recommendations

The following table summarizes Honeywell’s recommendations for IP address range selections. Refer to the subsequent sections for details on IP address requirements and examples for different LAN configurations.

LAN description	Recommendation
Isolated FTE community	Follow the best practices of connected communities so that if a router is needed later, the IP addresses have already conformed to Honeywell’s best practices.
Multiple FTE communities isolated from level 4 networks	<ul style="list-style-type: none"> <li>• Private IP addresses</li> <li>• Simple address range configuration</li> </ul>
FTE communities connected to level 4 with no COM communications	<ul style="list-style-type: none"> <li>• Private IP addresses with a firewall that performs Network Address Translation (NAT) for communication outside the plant control network.</li> <li>• Dedicated equipment for the firewall.</li> <li>• Placement of servers in a separate range from other Level 2 nodes.</li> </ul>
FTE communities connected to level 4 with COM communications	<ul style="list-style-type: none"> <li>• Unique level 2 and level 3 addresses that are compatible with level 4 addresses.</li> <li>• Does not use NAT.</li> <li>• A method that conserves addresses, although it is difficult to configure.</li> <li>• A subnet size that covers all level 2 nodes.</li> <li>• A server range contained in the lower addresses that allows the other level 2 nodes to start on a power of 2 boundaries.</li> <li>• A reserved subnet size that can be used for the largest level 1 range in the plant.</li> </ul>



### 8.1.3 IP addresses for non-Honeywell nodes

To prevent duplicate IP addresses on non-Honeywell nodes such as controllers, Honeywell recommends DHCP or BootP be used for IP addressing. Duplicate IP addresses on controllers lead to loss of process view.

### 8.1.4 Duplicate IP addresses

A Honeywell device performs a duplicate IP address check before joining the network, and after system startup. The Honeywell device does not join the network if a duplicate IP is detected. Honeywell devices include the following FTE or Ethernet resident controllers and interfaces.

- FTEB
- C300
- FIM4
- PGM2
- WSG
- HC900
- SM
- ENIM/EHPM
- ETN

A third-party device may not perform a duplicate IP address check. If a device does not perform a duplicate, this causes loss of communication if the device is configured with a static IP address in use by another device on the network. Third-party devices include any Ethernet resident, non-Honeywell devices, such as laptop, PDA, or a third-party embedded controller using Modbus TCP.

### 8.1.5 Best practices for preventing duplicate IP addresses

The following best practices are used to prevent duplicate IP addresses on the network.

- Allocate static IP addresses outside the embedded FTE IP address range. For example, if your base embedded FTE IP address range starts at 192.168.0.0/255.255.0.0, embedded controllers may be assigned addresses starting with 192.168.0.X or 192.168.1.X. Do not allocate any static IP addresses in this range. A “split subnet” topology can be used, where embedded controllers and servers exist on two different subnets.
- Use dynamic IP addresses for wireless laptops, PDAs, and other mobile devices. Devices that are frequently added and removed from the network, such as wireless laptops and PDAs, can be configured to use dynamic IP addresses from a DHCP server. The DHCP server must be configured with a dynamic IP address range that does not overlap the embedded FTE IP address range or any statically assigned IP addresses.

### 8.1.6 Recovering from a communication loss due to a duplicate IP address

The following procedure is used to recover from a communication loss due to a duplicate IP address.

1. Remove the third-party device from the network. Communication with the Honeywell device automatically recovers after the duplicate IP address is resolved. If communication does not recover within 5 minutes, proceed to the next step.
2. Perform a redundancy switchover of the Honeywell device (redundant, primary devices only). A redundancy switchover is commanded through the secondary device or invoked by physically resetting the primary device. Communication with the Honeywell device recovers after the new primary device joins the network after the switchover. If communication does not recover immediately following the switchover, wait for the redundant pair to synchronize and perform a second switchover. If communication does not recover immediately following the second switchover, proceed to the next step.

3. Physically reset the Honeywell device. Communication with the Honeywell device recovers after the device restarts.



**CAUTION**

Physically resetting the device causes all local control to cease execution.

---

## 8.2 Recommendations for FTE Network Communities

### Related topics

“Isolated FTE community” on page 59

“Multiple FTE communities isolated from Level 4 networks” on page 59

“FTE Communities connected to Level 4 with NO COM communications” on page 59

“Private address distribution ranges” on page 59

“FTE communities connected to level 4 with COM communications” on page 60

### 8.2.1 Isolated FTE community

IP address ranges and rules must follow the best practices of the multiple isolated or communities connected to level 4, even if there is complete isolation of the control LAN from the IT LAN. If the network expands to accommodate a router later, the IP addresses would have already conformed to Honeywell’s best practices for connected networks.

### 8.2.2 Multiple FTE communities isolated from Level 4 networks

Plant-wide networks contain several FTE communities connected by routers. If this network arrangement is isolated from the IT LAN, Honeywell recommends that private IP addresses be used. For ease of configuration, a simple address range of 10.CN.X.Y must be used for IP address distribution as described in the following table.

Octet	Description	Example
CN	FTE community number	First FTE subnet is 10.1.X.Y
CN	Multiple FTE communities can be connected with a router.	Second FTE subnet is 10.2.X.Y

### 8.2.3 FTE Communities connected to Level 4 with NO COM communications

For a plant-wide network that has a level 3 network connecting multiple FTE communities and other plant Ethernet based nodes, Honeywell recommends that private IP addresses with Network Address Translation (NAT) for communication with level 4 be used. NAT can be accomplished using a firewall. Honeywell recommends dedicated firewall equipment from Cisco. A Windows-based PC with firewall software is NOT recommended.

### 8.2.4 Private address distribution ranges

An IP address range of 10.CN.X.Y is used for private address distribution similar to that used for “**Multiple FTE communities isolated from level 4 networks.**” The following table describes the address ranges.

Octet	Description	Example
CN	FTE community number	<ul style="list-style-type: none"> <li>First FTE subnet is 10.1.X.Y</li> <li>Second FTE subnet is 10.2.X.Y</li> </ul>
X	<ul style="list-style-type: none"> <li>Range of addresses where the two types of nodes exist.</li> <li>Servers must be in a separate range from other Level 2 nodes.</li> </ul>	<ul style="list-style-type: none"> <li>10.1.0.Y for server nodes</li> <li>10.1.1.Y for station nodes</li> <li>10.1.2.Y for any other nodes such as ACE, PHD and third-party IP based nodes.</li> </ul>
Y	Any address between 1 and 255	10.1.2.24

**Using the previous examples**

Description	Exmample
If the FTE community is connected to a router, the router interface IP address must be in the same range as the servers.	10.1.0.1 for the router interface IP address. If the server is configured in the 10.1.0.Y range.
Level 1 nodes must be in the address space above the other nodes on level 2 and beyond the range of the subnet mask of the router interface, but within the subnet mask of the nodes that communicate.	<ul style="list-style-type: none"> <li>Level 1 addresses appear in the 10.1.4.Y range.</li> <li>Level 3 nodes must not communicate with level 1 nodes. The nodes have the following subnet masks. <ul style="list-style-type: none"> <li>Level 2 servers and Console stations with communication to level 1 nodes: 255.255.248.0.</li> <li>Level 2 nodes with no communication to level 1 nodes: 255.255.252.0.</li> <li>Level 1 controller nodes: 255.255.248.0.</li> <li>Level 3 router interface to level 2: 255.255.252.0.</li> </ul> </li> </ul>

**8.2.5 FTE communities connected to level 4 with COM communications**

When COM must communicate between level 4 and level 2, the level 2/level 3 addresses must be unique and compatible with level 4 addresses, and NAT cannot be used. OPC is an example of this type of communication. To minimize the number of corporate IP addresses used, an alternate method to the sparsely populated subnets used in the previous addressing scheme must be used. Although it is difficult to configure, Honeywell recommends a method that conserves addresses, such as the following:

- Obtain a subnet size that covers all the level 2 nodes.
- Contain the server range in the lower addresses and allow the other level 2 nodes to start on a power of 2 boundaries.

This is necessary so that the ACL filter used in the router to limit full access to the server nodes can be configured with a subnet mask that defines the server range.

**Example: FTE communities connected to Level 4 with COM**

The following table lists examples of the IP address distribution of an FTE community subnet containing the following:

- 5 servers
- 10 stations
- 2 ACE nodes
- 10 terminal servers
- 10 controllers with FTEB

A range of addresses are obtained from the corporate range, which is 164.1.0.0 for this example, with enough addresses for 126 nodes, the subnet default gateway and the subnet broadcast address. The address distribution is as follows:

IP address	Description
164.1.0.1	The router VLAN IP address with subnet mask of 255.255.255.192. Sufficient for 62 usable nodes, the subnet mask and the subnet broadcast address.
164.1.0.2-15	<ul style="list-style-type: none"> <li>Server nodes and some spare addresses.</li> <li>The subnet mask is 255.255.255.128 to cover both level 2 and level 1 nodes.</li> </ul>
164.1.0.16-63	<ul style="list-style-type: none"> <li>Stations, ACE terminal servers and some spare addresses.</li> <li>The subnet mask is 255.255.255.128 to cover the level 2 and level 1 nodes.</li> </ul>

IP address	Description
164.1.0.64-127	<ul style="list-style-type: none"><li>• FTEB (controller addresses must be outside of the subnet mask of the router interface).</li><li>• The subnet mask is 255.255.255.128 to cover the level 1 and level 2 range.</li><li>• The router interface to the FTE community blocks all access from level 3 by the subnet mask of 255.255.255.192.</li></ul>

## 8.3 Reusing IP Addresses for Level 1

### Related topics

“Purpose” on page 62

“Address reuse scheme for level 1” on page 62

“Route add command” on page 62

“Interface metric for non-FTE nodes” on page 63

### 8.3.1 Purpose

Level 1 devices consumes thousands of IP addresses in a corporate IP address space. To conserve corporate IP addresses, there is a scheme for reusing IP addresses. However, this scheme, must be used only if IP address reuse is necessary and private IP addresses are not available.



#### Attention

Do not use this scheme for standard network addressing.

### 8.3.2 Address reuse scheme for level 1

The following list summarizes the recommendations for an address reuse scheme.

- Only one range of address for level 1 must be requested from the corporate pool.
- This range can be reused in other FTE communities that are separated by a router.
- The address range must be large enough to accommodate all current and future level 1 nodes on this subnet.
- If a subnet is added with a larger number of level 1 nodes than the original range, a new range must be requested from the corporate pool.



#### Attention

Existing level 1 nodes do not need to have their addresses changed.

- With the addition of static routes in Experion R210 SP2 and Experion R400, private addresses such as 10.x.x.x or 192.168.x.x are used for this reused address range.

### 8.3.3 Route add command

Certain configurations must be implemented for level 2 nodes to communicate with level 1 nodes in the reusable address space. these configurations includes the use of the route add command and proper use of address ranges.

#### Route add command service

Experion R400 includes a service with Experion servers, direct consoles and ACEs to automatically insert an added route. The service runs on node startup and queries the server for the address range and subnet mask of the controllers. If the address of the node running the service is not in the range of the controllers, the static route to the controller is added to the yellow interface. The service tests for changes in the server database and to verify whether the static route is still connected to the yellow interface, every ten minutes. The errors and issues are sent to the application event log.

#### Static route add command

For level 2 nodes of ExperionR300 and earlier that must communicate with level 1 nodes in the reusable address space, a “route add” command must be configured in each level 2 node manually or by using a batch

file that runs at node startup. Nodes that do not communicate with the level 1 nodes do not need the “route add” configured.

---

The following example shows the command for a level 2 node in which the IP address range of level 1 and level 2 nodes are as follows:

- Level 2 address range is 164.1.0.0 to 164.1.7.255
- Level 1 address range is 164.0.0.0 to 164.0.2.255

Example: route add 164.0.0.0 mask 255.255.252.0 164.1.3.10 -p

**where**

- 164.0.0.0 is the base address of the level 1 subnet programmed in Control Builder.
  - 255.255.252.0 allows 1024 Level 1 FTE nodes.
  - 164.1.1.10 is the yellow interface IP addresses of the node being configured with the route add.
  - -p makes it persistent across reboots.
- 

**Results of route add command**

The level 1 nodes receive the address range of the level 1 nodes and the level 2 nodes. The level 1 nodes then calculate and add a static route to their IP stack to enable communication with level 2, using the above example.

- If the level 2 address range is 164.1.0.0 – 164.1.7.255
- The level 1 range in the Route Add example starts at 164.0.0.1.
- A subnet mask of 255.0.0.0 can be set in level 1 nodes through Control Builder and communications are open to the level 2 addresses.
- The range can be larger than the actual level 2 address range because communications will not go beyond the FTE community subnet.

### 8.3.4 Interface metric for non-FTE nodes

Experion servers, consoles or ACE nodes that do not run FTE must have the interface metric on the TCP/IP properties used for Experion communication set to 1.

To change or verify the setting, perform the following steps:

1. Click **Advanced** from the **TCP/IP Properties** dialog box.
2. Select the **IP Settings** tab.
3. Set the Interface Metric to **1**.





## 9 Installing and Replacing Switches

### Related topics

“Introduction” on page 66

“Installing and Configuring Cisco Switches” on page 67

“Replacing Switches” on page 70

“Stacking Switches” on page 72

“Honeywell control firewall” on page 76

“Honeywell’s switch configuration files” on page 78

“Configuring Cisco switches” on page 89

“Saving and modifying Cisco switch configuration files” on page 103

“Updating the Honeywell control firewall firmware” on page 105

---

## 9.1 Introduction

### Related topics

“Prerequisites” on page 66

“Qualified network equipment for use in an FTE network” on page 66

### 9.1.1 Prerequisites

Ensure that the following requirements are met before performing the procedures in this section.

Status	Task
	Awareness of all FTE requirements and configuration rules in addition to any specific site and networking requirements.
	Planned your FTE System including the use of firewalls.
	Verified platform requirements have been met.
	Reviewed the Fault Tolerant Ethernet (FTE) Experion Specification and Technical Data.
	Reviewed the Software Change Notice (SCN) for your release, which provides last-minute changes, special instructions, and workarounds.
	Verify the switches have the IOS version qualified by Honeywell as listed in the Software Change Notice. <b>Note:</b> If the version is not the same as that listed in the SCN, contact Honeywell Network Services for the procedure to upgrade the IOS.

### 9.1.2 Qualified network equipment for use in an FTE network

For a list of qualified switches and other network equipment, refer to the latest Experion Platform Fault Tolerant Ethernet (FTE) Specification and Technical Data.

## 9.2 Installing and Configuring Cisco Switches

### Related topics

- “FTE switch installation guidelines” on page 67
- “Configuring Cisco switches to prevent storms” on page 67
- “Expanding an existing FTE network” on page 67
- “Using spanning tree” on page 68
- “Ciscoswitch port and connection speeds” on page 68

### 9.2.1 FTE switch installation guidelines

The following table provides an overview of the Ethernet switch requirements and guidelines.

Subject	Requirement/guideline
Highest level	Two switches (one for the <i>Yellow</i> tree and one for the <i>Green</i> tree) are required at the highest switch level and they <b>MUST</b> be interconnected.
Tree level	Two switches (one for the <i>Yellow</i> tree and one for the <i>Green</i> tree) are required to maintain redundancy.
Small FTE network	Consists of only one level of switches.
Large FTE network	Consists of intermediate level of switches in addition to the grouping and backbone level switches, depending on the plant topology.
Number of switch ports	The Honeywell qualified Cisco 3750 switch are expanded in increments of 12 ports, up to a maximum of 96 ports.

### 9.2.2 Configuring Cisco switches to prevent storms

The addition of controllers to the FTE community requires an increased level of reliability and security. Cisco switches, when properly configured, provide this increased performance by limiting potentially damaging traffic conditions known as *storms*. Switches must be configured to limit multicast, broadcast, and unicast traffic at the ingress to the switch to 20 percent of total bandwidth for 100-Megabit connections. When the traffic into a port goes above the limit, it is disconnected. When it drops below 18 percent, communication is restored.

For new switches qualified with R400, storms are applied using Mbps measures instead of percentage filtering. 20 Mbps is applied on interfaces level 2 with 18 Mbps as the restore limit. Limits for level 1 nodes and uplinks are 1 Mbps (0.8 recovery) broadcast and 2 Mbps (1.8 recovery) multicast. Furthermore, *bpduguard* is now configured on all non-uplink interfaces to disable loops and prevent unexpected uplink placement.

### 9.2.3 Expanding an existing FTE network

You can continue to use Nortel switches if they are already installed. However, controller nodes must be connected to qualified Cisco switches, and cannot be connected to Nortel switches. The addition of a controller to any FTE network also requires the addition of Cisco switches to maintain the level of reliability and security necessary for controller-server, controller-station and controller peer-peer communication.

Current installations with Nortel switches that are expanding must purchase Cisco switches for the new nodes.

#### Switch hierarchy

If you are using Nortel and Cisco switches in the same network, Cisco switches must be at the top of the switch hierarchy and the Nortel switches must connect into the Cisco switches.

## 9.2.4 Using spanning tree

Spanning tree must be enabled on Cisco switches to increase protection against accidental creation of a loop in the switch tree. Potential loss of view and control occurs if a loop is created in the switches with controllers in the system. This increased protection is critical. Furthermore, *BPDUGuard* is configured on non-uplink interfaces to prevent loops. Spanning tree must remain disabled for existing Nortel switches in an FTE community.

To make the spanning-tree behavior deterministic, the top level yellow switch must be configured with the highest spanning-tree root priority and the top level green as the second highest. The FTE crossover cable must be connected between these two switches.

### Setting up the root pair of FTE Switches when configuring the network

To setup the root pair of FTE Switches while configuring the network, you must ensure that the appropriate commands are used in the switch configuration files.

It is recommended to manually apply these commands to the top level switch pair in the FTE network.

Ensure that one of the following commands are used for the top level switch pair, before loading the updated switch configuration files to the FTE network.

```
For the top level Yellow switch
!Uncomment the following line only if this is the top level Yellow switch
!spanning-tree mst 0 priority 4096 !
```

```
For the top level Green Switch.
!Uncomment the following line only if this is the top level Green switch
!spanning-tree mst 0 priority 8192
```

If the switch has already had its configuration loaded perform these commands on the appropriate switch:

```
Go into enable mode for the Cisco Switch perform the following steps for the top Yellow switch:
config t
spanning-tree mst 0 priority 4096
end
write
Go into enable mode for the Cisco Switch perform the following steps for the top Green switch:
config t
spanning-tree mst 0 priority 8192
end
write
```



#### CAUTION

To prevent loss of network communication, you must use caution while making any changes to your spanning tree protocol. For example, if you change from PVST to MST, all switches in the network tree are temporarily blocked until spanning tree is recalculated.

## 9.2.5 Ciscoswitch port and connection speeds

The following table summarizes the switch port and connection speeds for the Cisco switch.

Switch port	Requirement	Comment
Level 1 controller	<ul style="list-style-type: none"> <li>Port fast spanning tree enabled.</li> <li>Must have the speed set to <i>auto</i> with <i>full duplex</i>.</li> </ul>	Allows quick reconnection
Level 2 100 Megabit nodes	<ul style="list-style-type: none"> <li>Port fast spanning tree enabled.</li> <li>Must have the speed set to <i>100 Megabit</i> and <i>full duplex</i>.</li> </ul>	Allows quick reconnection

Switch port	Requirement	Comment
Uplink/downlink ports	<ul style="list-style-type: none"> <li><i>Normal</i> spanning tree enabled</li> <li>Must have the speed set to <i>100 Megabit</i> and <i>full duplex</i>.</li> </ul>	<ul style="list-style-type: none"> <li>Cisco does not recommend using this feature when connecting to other switches.</li> <li>The exception is the GBIC based ports, which do not have the problem of locking on the wrong speed or duplex.</li> </ul>
Ports connected to Microsoft based nodes	<ul style="list-style-type: none"> <li><i>Port fast</i> spanning tree enabled.</li> <li>Must have the speed set to <i>100 Megabit</i> and <i>full duplex</i>.</li> </ul>	Additionally, NIC cards in Microsoft software based nodes must also have the speed set to 100 Megabit and full duplex.
Switch ports connected to FTEB nodes	Must have the speed set to <i>auto</i> and the duplex set to <i>full</i> .	

### Implementing the Cisco switch port configurations

To make the Cisco switch configuration repeatable and predictable, Honeywell provides a set of configuration files to be used for different switch configuration options. Information about and procedures for using these configuration files are included in Section 9.6.

### Connecting switches

Switches must be connected to either the interfaces configured as uplinks or to GBIC based interfaces. Uplinks (or downlinks) must NOT be connected to interfaces configured for FTEB or 100 Megabit Level 2 node connections.

### Switch power source



#### Attention

Redundant Ethernet switches must NOT be connected to the same AC power source.

---

## 9.3 Replacing Switches

### Related topics

“Upgrading the switch” on page 70

“Guidelines for replacing FTE switches” on page 70

“Special considerations for replacing stacked switches” on page 70

“Tasks for configuring and replacing switches” on page 70

### 9.3.1 Upgrading the switch

It is recommended that the user update the IOS versions and configurations with the latest version. Both switches in a yellow/green switch pair must be loaded with the same IOS and configuration, if possible. It is recommended that you contact Honeywell Network Services to determine the risk of network configuration changes against the security and fault mitigation enhancements provided by the latest files.

### 9.3.2 Guidelines for replacing FTE switches

Following are guidelines for replacing switches in an FTE network.

- All switch pairs must be the same make and model number. For example switch A and switch B must both be a Cisco 3750G-12S.
- Before beginning the replacement procedures, configure switches offline using the switch configuration files provided by Honeywell.
- If you are replacing both switches, replace switch B, followed by switch A.
- Ensure that the switch replaced first is operating properly before replacing the second switch.
- If you are replacing a switch in a stacked configuration, follow the guidelines in Section 9.4, “Stacking Switches.”

### 9.3.3 Special considerations for replacing stacked switches

3750-12s switches that are stacked, have a vulnerability while replacing a failed switch in the stack. The problem is fixed in IOS release 12.2(25)SEE2. Honeywell qualifies the IOS version for stacked switches and identifies the correct version in the Software Change Notice (SCN) for your release. If the replacement switch’s IOS is not the same as the one identified in the SCN included with your system, you must upgrade the IOS before you begin the replacement.

When you power up the switch, the IOS spreads to the other switches in the stack. After the replacement switch stack is backed up and running, you must also upgrade the IOS on the companion switch stack in the network to keep the IOS the same on the FTE switch stack pair.

Consult Honeywell Network Services for the procedure to upgrade the IOS. The IOS upgrade image is available from Honeywell TAC or Cisco and has the following requirements.

- The IOS upgrade image must be the IP base with web services support.
- You must use the IOS upgrade image file with a .tar extension. Using the .bin file results in the switch not spreading the new IOS to the other switches in the stack.

### 9.3.4 Tasks for configuring and replacing switches

Following is a list of tasks to perform while replacing switches.

Task	Action
Configure new switch A-yellow (offline)	<ul style="list-style-type: none"> <li>• See “Connecting locally to the switch” on page 112.</li> <li>• Verify the switches have the IOS version qualified by Honeywell as listed in the SCN for your release.</li> </ul> <hr/> <p><b>! Attention</b> If the version is not the same as that listed in the SCN, contact Honeywell Network Services for the procedure to upgrade the IOS.</p> <hr/> <ul style="list-style-type: none"> <li>• See “Configuring switch interface options” on page 113.</li> <li>• See “Loading the switch configuration file” on page 121.</li> </ul>
Configure new switch B-green (offline)	<ul style="list-style-type: none"> <li>• See “Connecting locally to the switch” on page 112.</li> <li>• Verify the switches have the IOS version qualified by Honeywell as listed in the SCN for your release.</li> </ul> <hr/> <p><b>! Attention</b> If the version is not the same as that listed in the SCN, contact Honeywell Network Services for the procedure to upgrade the IOS.</p> <hr/> <ul style="list-style-type: none"> <li>• See “Configuring switch interface options” on page 113.</li> <li>• See “Loading the switch configuration file” on page 121.</li> </ul>
Install new switch B-green	<ul style="list-style-type: none"> <li>• If necessary, label network cables with the switch port type they are connected to.</li> <li>• Shut down existing switch B green.</li> <li>• If switch pair is not at the top level, remove the uplink cable from existing switch B green.</li> <li>• If switch pair is at the top level, remove the crossover cable from existing switch B green.</li> <li>• Disconnect network cables from switch B green.</li> <li>• If switch pair is not at the top level, connect the uplink cable to the new switch B green.</li> <li>• Connect network cables to the new switch B green verifying you are connected to the correct switch port type.</li> <li>• If switch pair is at the top level, connect crossover cable to the new switch B green.</li> <li>• Turn on switch B green and verify the new switch B green is communicating.</li> </ul>
Install new switch A-yellow	<ul style="list-style-type: none"> <li>• Shut down existing switch A yellow.</li> <li>• If switch pair is not at the top level, remove the uplink cable from existing switch A yellow.</li> <li>• If switch pair is at the top level, remove the crossover cable from existing switch A yellow.</li> <li>• If necessary, label network cables with the switch port type they are connected to.</li> <li>• Disconnect network cables from existing switch A yellow.</li> <li>• If switch pair is not at the top level, connect the uplink cable to the new switch A yellow.</li> <li>• Connect network cables to new switch A yellow verifying you are connected to the correct switch port type.</li> <li>• If switch pair is at the top level, connect crossover cable to the new switch A yellow.</li> <li>• Turn on switch A yellow and verify the new switch A yellow is communicating.</li> </ul>

## 9.4 Stacking Switches

### Related topics

“About stacked switches” on page 72

“Tasks for stacking switches” on page 72

“Checking the switch IOS” on page 73

“Modifying the stacked switch configuration files” on page 74

“Configuring switch priority in a stacked switch” on page 75

### 9.4.1 About stacked switches

A stacked switch configuration allows two or more switches to be clustered in a way that they function and appear as one switch on the network. A true stacked switch configuration is different from connecting switches through the uplink ports to provide additional ports. The 3750 switches qualified by Honeywell are truly stackable switches and act as one logical unit when connected through the backplane with the special cable. Up to nine 3750 switches can be stacked. The following figure shows two separate switch configurations, each of which is comprised of three stacked switches. The first, third and fifth switches comprise the *yellow* switch and the second, fourth and sixth switches comprise the *green* switch.



### 9.4.2 Tasks for stacking switches

Switches can be stacked either by connecting a new switch to an existing switch, or by connecting two new switches and adding the stacked switch to the network. Following are the tasks associated with stacking switches in an FTE network.

1. Power up and connect to the first base switch. See “Connecting locally to the switch” on page 112.
2. Verify the switches have the IOS version qualified by Honeywell as listed in the SCN for your release. If the version is not the same as that listed in the SCN, contact Honeywell Network Services for the procedure to upgrade the IOS.



**CAUTION**

The first switch in the stack must have the correct Internal Operating System (IOS) and the switches added to the stack must not have an IOS newer than the qualified version.

3. Configure the base switch. See “Configuring switch interface options” on page 113.
4. Load the switch configuration file on the base switch. See “Loading the switch configuration file” on page 121.
5. Power up the next switch to be added to the stack (do not connect it at this time) and verify whether it has the correct IOS version. See “Checking the switch IOS” on page 90.
6. Power down the switch and then connect it to the stack. See the 3750-12s User Manual for connection procedures.

**CAUTION**

Ensure that you verify whether the switch is powered off before connecting it to the stack. Connecting a switch that is powered on causes other switches to reload and change their configuration.

7. Add the switch to the stack by typing the following commands at the switch prompt, substituting the switch number in the stack for X.

```
Conf t
Switch x provision ws-3750-12
```

For example:

- C3750-G1#Conf t
- C3750-G1#Switch 3 provision ws-3750g-12

**Attention**

Switch provisioning allows you to configure each switch in the stack with a separate configuration.

8. Edit the `v101_stack.txt` switch configuration file for the switch being added. See “Modifying the stacked switch configuration files” on page 90.
9. Load the new switch configuration file to the stacked switch. See “Loading the switch configuration file” on page 121.
10. Repeat tasks 5 through 9 until all switches in the stack are added, making sure each new switch is fully loaded before adding the next one.
11. When all switches in the stack are fully loaded and ready, issue a show switch command to the base switch.

For example: C3750-G1#show switch

Current switch state	Role	MAC address	Priority
* 1 Ready	Master	0015.faa3.8800	3
2 Ready	Member	0015.faa3.bf00	2
3 Ready	Member	0017.94b2.6800	1

All switches in the stack must indicate **Ready** status.

12. Configure the switch priority to increase the chances the base switch remains the master switch. See “Configuring switch priority in a stacked switch” on page 92.

### 9.4.3 Checking the switch IOS

Cisco’s IOS version checking software detects the IOS version of each switch in the stack and updates all switches to the latest version available, which may not be the version qualified by Honeywell. Switches with an unqualified IOS have unpredictable performance. Use this procedure to check the IOS version.

1. Use the Switch Configuration Tool's Serial or Telnet connection to verify the switch's IOS version. You can also install the Tera Term application from the Experion PKS Installation media on an Experion PKS computer.
2. Enable and log in to the switch.
3. Check the IOS version by typing the following command at the switch prompt.

```
show boot
```

For example:

```
c3750-g1#show boot
BOOT path-list : flash:c3750-ipbase-mz.122-25.SEE2/c3750-ipbase-mz.122-25.S
```

The IOS version in the above example is 122-25.SEE2

4. For more information, refer to the IOS version qualified by Honeywell as listed on the Honeywell Process Solutions website (<http://www.honeywellprocess.com/library/support/software-downloads/Customer/FTE-Qualified-IOS-Firmware-for-Cisco-Switches.pdf>).



#### Tip

The IOS upgrade image is available from Honeywell TAC or Cisco.

- The IOS upgrade image must be the IP base with web services support.
- You must use the IOS upgrade image file with a *.tar* extension. Using the *.bin* file results in the switch not spreading the new IOS to the other switches in the stack.

## 9.4.4 Modifying the stacked switch configuration files

Honeywell provides a default stacked switch configuration file (V101\_stack) that can be modified to configure additional switches and options. See Section 9.7 for procedures on using switch configuration files. Use this procedure to modify the stacked switch configuration file and reuse it.

1. Copy the *v101\_stack.txt* file to a location where you can edit it.
2. Rename the file according to the switch order in the stack.

For example, use *v101\_stack3.txt* for the third switch in the stack.

3. Identify the switch order in the interface range command.

```
interface range GigabitEthernet2/0/1 - 12
```

For example, change the 2 following Gigabit Ethernet to a 3 to identify the third switch in the stack.

```
interface range GigabitEthernet3/0/1 - 12
```



#### Attention

- You can also edit the 1 – 12 to a different range of ports to be configured as Gigabit.

4. Identify the VLAN to be used in the switchport access command.

```
switchport access vlan 101
```

For example, change 101 to 102

```
switchport access vlan 102
```

5. Save the file to a location from which you can access it using Tera Term's Xmodem file transfer utility.

**Tip**

The IOS upgrade image is available from Honeywell TAC or Cisco.

- The IOS upgrade image must be the IP base with web services support.
- You must use the IOS upgrade image file with a .tar extension. Using the .bin file results in the switch not spreading the new IOS to the other switches in the stack.

## 9.4.5 Configuring switch priority in a stacked switch

Configuring the switch priority increases the chances of the base switch to remain the master switch. Perform the following procedure to establish specific priority for each switch in the stack.

1. Serial connect or telnet to the switch.
2. Enable and log in to the switch.
3. Type the *Conf t* at the switch prompt.
4. Type *Switch X priority XX* at the switch prompt, substituting the switch number for X and the priority order for XX.

**Attention**

- The higher the number used for XX, the higher the priority.

In the following example, Switch 1, which is configured as the base switch, has the highest priority.

```
C3750-G1#Conf t
C3750-G1#Switch 1 priority 15
C3750-G1#Conf t
C3750-G1#Switch 2 priority 14
C3750-G1#Conf t
C3750-G1#Switch 3 priority 13
```

**For additional information**

- See Table 9-4 for a comprehensive list of all Honeywell's switch configuration files.
- See Section 11.4 for additional examples of stacked switch configuration files.

## 9.5 Honeywell control firewall

The Honeywell control firewall provides security and determinism for level 1 FTE nodes. These switches connect to uplink ports and only support level 1 nodes. For further details on planning, installation and configuration of the Honeywell Control Firewall, refer to the *Honeywell Control Firewall User's Guide*.

### Related topics

“Honeywell control firewall connection requirements” on page 76

“Honeywell control firewall guidelines” on page 76

“Benefits of Honeywell control firewalls” on page 77

### 9.5.1 Honeywell control firewall connection requirements

The following are the connection requirements for a Honeywell control firewall

- All FIM4s and C300s must connect to a Honeywell control firewall.
- Any FTEBs to which a C300 communicates, must connect to the same Honeywell control firewall as the C300.
- C200/FTEB and FIM/FTEB may connect to level 1 configured switches according to the established best practices or to a Honeywell control firewall.
- The Honeywell control firewall uplink port must always connect to a Cisco switch.
- The Honeywell control firewall must not be stacked.
- The Honeywell control firewall must be connected to an interface configured for portfast.

### 9.5.2 Honeywell control firewall guidelines

Connect Honeywell control firewalls to switch interfaces configured for level 2 host nodes or interfaces a computer is connected, and configure the interface as follows:

- Type: portfast
- Type speed: 100
- Type duplex: full
- Broadcast 20 megabit
- Multicast 20 megabit

If you connect a Honeywell control firewall to a top level switch such as a 3750 configured for all uplink ports, verify the control firewall interface is configured for portfast.

ensure that no other connections of Cisco to Cisco switches are configured for portfast – only those used for Honeywell control firewalls.

#### Preventing loss of view in the Honeywell control firewall



#### CAUTION

- Recovery of a root switch in a network causes recalculation of the switch spanning tree topology. As Honeywell control firewalls do not use spanning tree, interfaces connected to control firewalls are blocked and cause loss of view unless the interfaces are set to portfast.
- Configure all Honeywell control firewall interfaces for portfast before attaching the control firewall.
- Do not connect control firewalls to interfaces configured for uplinks.

### 9.5.3 Benefits of Honeywell control firewalls

A Honeywell Control Firewall provides the following benefits.

- Blocks messages that level 1 nodes must not receive, and throttles Ethernet management messages to those nodes.
- Has similar but stronger protection than a level 1 configured Cisco switch.
- Can connect to any Cisco switch, configured for level 1 or level 2.
- An Experion R300 or later system with all control on the C300s and FIM4s connected through Honeywell control firewalls does not need any level 1 configured Cisco switches.
- Includes a switch with eight device ports and one uplink port. Its functions do not a switch in the FTE network limit of three levels of switches.
- Requires no management or configuration.
- Firmware can be easily updated using the Control Firewall Update Tool.

## 9.6 Honeywell's switch configuration files

Honeywell provides switch configuration files that, when implemented, configure the FTE switch ports for different node types according to defined requirements. Table 9-4 lists all available switch configuration files.

### Related topics

- “Location of switch configuration files” on page 78
- “Obtaining the latest switch configuration files” on page 78
- “Switch configuration requirements” on page 79
- “Configuring switches for network level communication” on page 79
- “Cisco switch and port options” on page 81
- “Configuration order for switch ports” on page 81
- “Switch configuration examples” on page 81
- “Details for switch configuration files” on page 83

### 9.6.1 Location of switch configuration files

Switch configuration files are available from the following locations.

- SSOL or Network Services – this location contains the newest switch files
- For Experion users, on the Experion PKS Installation media.
- For TPS users, on the TPS System Software media.

### 9.6.2 Obtaining the latest switch configuration files

Use this procedure to obtain the latest version of the switch configuration files from SSOL.

1. Type the following URL in a web browser.

<http://www.honeywellprocess.com>

2. Click **Login to My Account**.



#### Attention

- If you are a new user, register for access.

3. Type the user name and password, and then click **Login**.
4. Under **SUPPORT**, click **Security & Other Updates**.
5. Under **Security & Other Updates**, click **FTE Switches - Cisco**.
6. In the list, click the *Cisco\_Configuration\_xxx\_Download.zip*.
7. Save the *.zip* file to your local machine.
8. Double-click the downloaded *.zip* file to open it.
9. Read the *Important Notice.txt* file for recent update information.
10. Archive all existing switch configuration files.
  - a. Navigate to the following path.
 

```
Program Files\Honeywell\FTEDriver\SwitchConfigurationFiles\ Cisco Catlyst <Model of switch>
```
  - b. Rename the *Switch Configuration* folder to *Old Switch Configuration*.
  - c. Create a new *Switch Configuration* folder.
11. Run the switch configuration executable.
  - a. Double-click *Cisco\_Configuration\_MMMYY.exe*, where *MMYY* is the latest month and year of the file.
  - b. Click **Yes** if you receive a Win-Zip caution.

12. From the Win-Zip self extractor dialog, select C:\ drive as the default or select the drive where Honeywell software is installed.

All the switch configuration files are unzipped to the following location:

*Program Files\Honeywell\FTEDriver\SwitchConfigurationFiles*

### 9.6.3 Switch configuration requirements

The following table summarizes the FTE switch port configuration requirements for various node types.



#### Attention

- The following configurations apply to the newer model switches (2960, 3560, 3750, IE3000). In case you are using the 2950, 2955, and 3550 model switches refer to the R3xx configuration requirements.

Node type	Status	Duplex	Speed	Spanning tree
Uplink port	Enable	Full	100 Megabit	Normal spanning tree enabled
FTE Bridge	Enable	Full	Auto	Port fast spanning tree and BPDUguard enabled
FTE Node	Enable	Full	100 Megabit	Port fast spanning tree and BPDUguard enabled
SFP based ports	Enable		1 Gigabit	Normal spanning tree enabled
CF9	Enable	Full	100 Megabit	Port fast spanning tree and BPDUguard enabled.

### 9.6.4 Configuring switches for network level communication

The switch files provided by Honeywell allow you to configure specific communication parameters in the switches depending on the level of communication needed between the FTE network levels. Additionally, the files contain features to improve network security for level 1 nodes. The following table summarizes the configuration options set in the four types of switch configuration files.



#### Attention

- The following configurations apply to the newer model switches (2960, 3560, 3750, IE3000). If you are using the 2950, 2955, and 3550 model switches refer to the R3xx configuration requirements.

Network level	Requirements
Level 1 only	<p>To help protect against network problems, the level 1-only switches have the following tighter limits on incoming traffic.</p> <ul style="list-style-type: none"> <li>Uplink and GBIC inbound limits <ul style="list-style-type: none"> <li>Broadcast 1 Megabit</li> <li>Multicast 2 megabit for RJ45 interfaces</li> </ul> </li> </ul>
Level 2 only	<p>Level 2-only switches have the following configuration.</p> <ul style="list-style-type: none"> <li>Uplink, GBIC, and Level 2 Nodes: Inbound limits <ul style="list-style-type: none"> <li>Broadcast 20 megabit</li> <li>Multicast 20 megabit</li> </ul> </li> <li>Level 2 Nodes: Inbound prioritization: <ul style="list-style-type: none"> <li>CDA packets are given priority</li> </ul> </li> </ul>

Network level	Requirements
Mixed level 1 and level 2	<p>Mixed Level 1 and Level 2 configuration have the following configuration.</p> <ul style="list-style-type: none"> <li>• Uplink and GBIC inbound limits. <ul style="list-style-type: none"> <li>– Broadcast 1 megabit</li> <li>– Multicast 2 megabit for RJ45 interfaces</li> </ul> </li> <li>• Level 1 nodes - Inbound prioritization. <ul style="list-style-type: none"> <li>– CDA packets are given priority</li> <li>– Broadcast 1 megabit</li> <li>– Multicast 2 megabit</li> </ul> </li> <li>• Level 2 nodes: Inbound limits. <ul style="list-style-type: none"> <li>– Broadcast 1 megabit</li> <li>– Multicast 2 megabit</li> </ul> </li> </ul>
Split level 1 and level 2	<p>Split level 1 and level 2 configuration have the following configuration.</p> <ul style="list-style-type: none"> <li>• Uplink inbound prioritization <ul style="list-style-type: none"> <li>– CDA packets given priority</li> <li>– Broadcast 20 megabit</li> <li>– Multicast 20 megabit</li> </ul> </li> <li>• Level 1 nodes - inbound prioritization <ul style="list-style-type: none"> <li>– CDA packets given priority</li> <li>– Broadcast 1 megabit</li> <li>– Multicast 2 megabit</li> </ul> </li> <li>• Level 1 crossover uplink - inbound ACL filtering</li> <li>• Level 2 nodes - inbound limits <ul style="list-style-type: none"> <li>– Broadcast 20 megabit</li> <li>– Multicast 20 megabit</li> </ul> </li> </ul>
Network level	Requirements
Level 2 only	<p>Level 2-only switches have the following configuration.</p> <ul style="list-style-type: none"> <li>• Uplink, GBIC, and Level 2 Nodes: Inbound limits <ul style="list-style-type: none"> <li>– Broadcast 5000pkts/5 seconds</li> <li>– Multicast 5000pkts/5 seconds</li> </ul> </li> <li>• Level 2 Nodes: Inbound prioritization: <ul style="list-style-type: none"> <li>– CDA packets are given priority</li> </ul> </li> </ul>
Mixed level 1 and level 2	<p>Mixed Level 1 and Level 2 configuration have the following configuration.</p> <ul style="list-style-type: none"> <li>• Uplink and GBIC inbound limits. <ul style="list-style-type: none"> <li>– Broadcast 5000pkts/5 seconds</li> <li>– Multicast 5000pkts/5 seconds for RJ45 interfaces</li> </ul> </li> <li>• Level 1 nodes - Inbound prioritization. <ul style="list-style-type: none"> <li>– CDA packets are given priority</li> <li>– Broadcast 5000pkts/5 seconds</li> <li>– Multicast 5000pkts/5 seconds</li> </ul> </li> <li>• Level 2 nodes: Inbound limits. <ul style="list-style-type: none"> <li>– Broadcast 5000pkts/5 seconds</li> <li>– Multicast 5000pkts/5 seconds</li> </ul> </li> </ul>



### 9.6.5 Cisco switch and port options

After installing the redundant pair of switches, you must configure the Cisco switches using the switch's command line interface and the correct switch startup configuration file. Switch configuration files, which are copied to the hard disk when the FTE Mux Driver package is installed, configure the switch and port options as listed in the following table. Additionally, the configuration files contain Quality of Service parameters that are attached to the ports.

Option types	Available options	
Switch options	<b>Honeywell model</b> <ul style="list-style-type: none"> <li>• NE-SW224S</li> <li>• NE-SW248S</li> <li>• NE-SW224T</li> <li>• NE-SW248T</li> <li>• NE-SW312S</li> <li>• NE-SW324S</li> <li>• NE-SW512C</li> <li>• NE-SW504S</li> <li>• NE-SW508S</li> <li>• NE-SW3242S</li> <li>• NE-SW312X</li> <li>• NE-SW224P</li> <li>• NE-SW248P</li> <li>• NE-SW24G1</li> </ul>	<b>Cisco model</b> <ul style="list-style-type: none"> <li>• 2960-24TC-L</li> <li>• 2960-48TC-L</li> <li>• 2960-24TT-L</li> <li>• 2960-48TT-L</li> <li>• 3750G-12S-S</li> <li>• 3560-24TS-S</li> <li>• 2955C-12</li> <li>• IE-3000-4TC</li> <li>• IE-3000-8TC</li> <li>• 3560V2-24TS-S</li> <li>• 3750X-12S-S</li> <li>• 2960+24TC-L</li> <li>• 2960+48TC-L</li> <li>• 2960X-24TS-L</li> </ul>
Port configuration options	<ul style="list-style-type: none"> <li>• Number of uplink ports</li> <li>• Number of full duplex auto speed FTEB ports</li> <li>• Number of full duplex 100 Megabit ports</li> <li>• Whether the switch ports have VLAN101 configured.</li> <li>• Level 1 only, level 2 only, or level 1/level 2 split</li> </ul>	

### 9.6.6 Configuration order for switch ports

The specific configuration file you choose defines the switch options and how each switch port is configured. Uplink ports are configured first, FTE bridge ports are configured second, and FD-100 Megabit ports are configured third. The following table summarizes the switch port configuration settings.

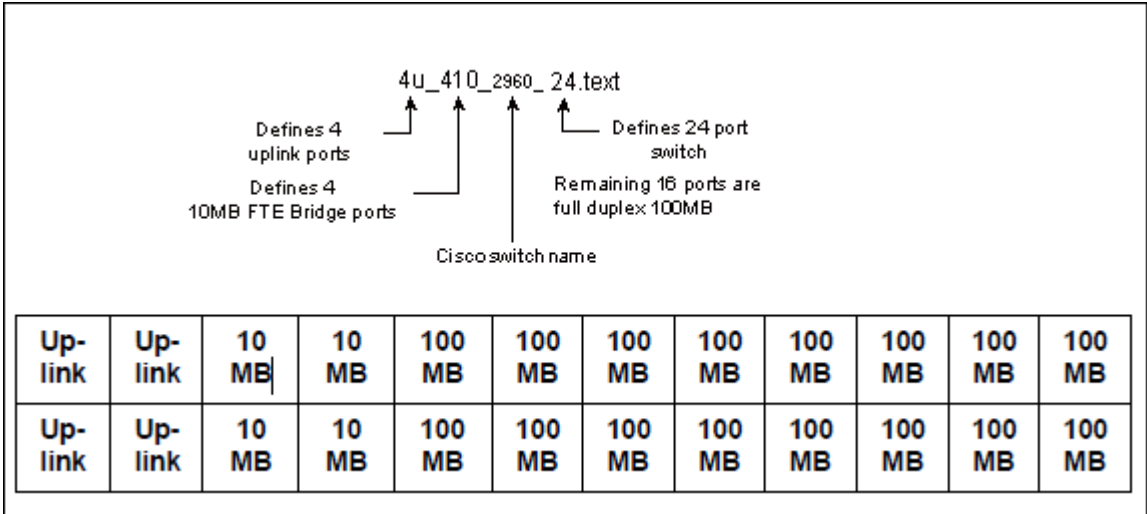
Configuration order	Port type	Spanning tree	Status	Duplex	Speed
1 <sup>st</sup>	Uplink ports	Enabled	Enable	Full	100 Mbps
2 <sup>nd</sup>	FTE bridge ports	Portfast/BPDUguard	Enable	Full	Auto
3 <sup>rd</sup>	FTE	Portfast/BPDUguard	Enable	Full	100 Mbps

### 9.6.7 Switch configuration examples

This section contains examples that illustrate how switch ports are configured using the switch configuration files.

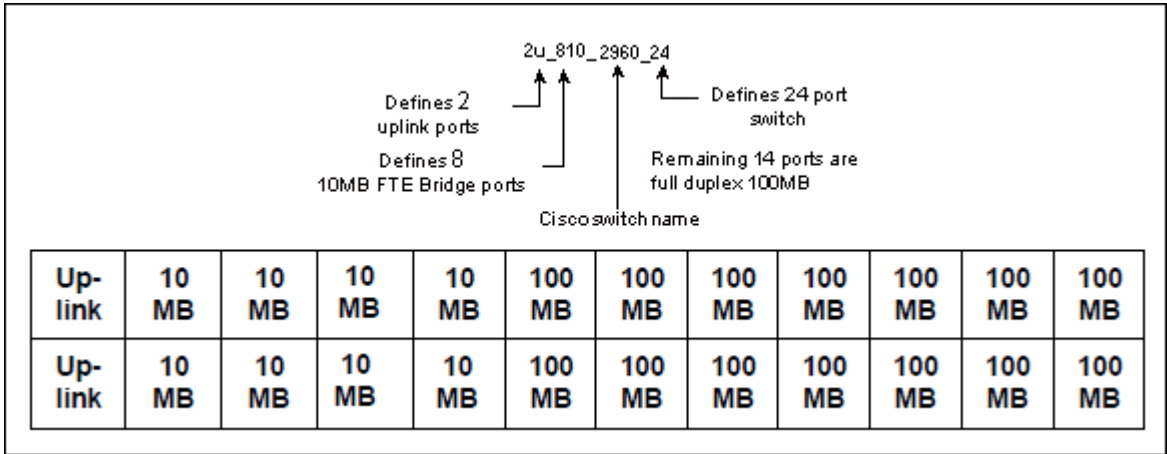
4u\_410\_24 switch configuration file

This file for the Cisco 2960-24 switch configures 4 uplink ports, 4 FTE Bridge ports and 16 100MB Full Duplex ports.



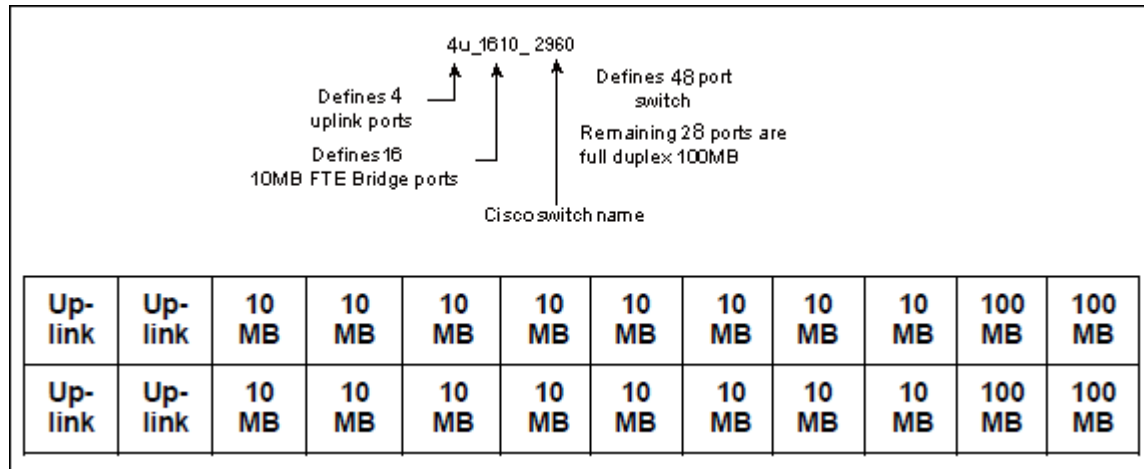
2u\_810\_Cisco2960\_24 switch configuration file

This file for the Cisco 2960 switch configures 2 uplink ports, 8 FTE Bridge ports and 14 FD 100 MB Full Duplex ports.



4u\_1610\_Cisco2960\_24 switch configuration file

This file for the Cisco 2960 switch configures 4 uplink ports, 16 FTE Bridge ports and 28 FD 100 MB Full Duplex ports.



### 9.6.8 Details for switch configuration files

The following table provides details on the specific parameters implemented in each switch configuration file. The Level column indicates the network level for which the switch configuration file must be used.

File name	Level	Switch type	Number of uplinks	Number of 10 MB FTEBs	Number. of FD 100 MBs	VLAN101 configured
<b>Cisco 2950</b>						
2u	2	2950-48	2	0	46	No
2u_24	2	2950-24	2	0	22	No
4u	2	2950-48	4	0	44	No
4u_24	2	2950-24	4	0	20	No
4u_410	1 and 2	2950-48	4	4	40	No
4u_410_24	1 and 2	2950-24	4	4	16	No
4u_810	1 and 2	2950-48	4	8	36	No
4u_810_24	1 and 2	2950-24	4	8	12	No
4u_1610	1 and 2	2950-48	4	16	28	No
4u_1610_24	1 and 2	2950-24	4	16	4	No
12u_24	2	2950-24	12	0	12	No
24u	2	2950-48	24	0	24	No
L1_1u_2310_24	1	2950-24	1	23	0	No
L1_1u_4710	1	2950-48	1	47	0	No
L1_2u_2210_24	1	2950-24	2	22	0	No
v101_2u	2	2950-48	2	0	46	Yes
v101_2u_24	2	2950-24	2	0	22	Yes
v101_4u_24	2	2950-24	4	0	20	Yes
v101_4u_410	1 and 2	2950-48	4	4	40	Yes
v101_4u_410_24	1 and 2	2950-24	4	4	20	Yes
v101_4u_810	1 and 2	2950-48	4	8	36	Yes
v101_4u_810_24	1 and 2	2950-24	4	8	12	Yes
v101_4u_1610_24	1 and 2	2950-24	4	16	4	Yes

File name	Level	Switch type	Number of uplinks	Number of 10 MB FTEBs	Number. of FD 100 MBs	VLAN101 configured
v101_12u_24	2	2950-24	12	0	12	Yes
v101_24u	2	2950-48	24	0	24	Yes
v101_4u	2	2950-48	4	0	44	Yes
v101_4u_1610	1 and 2	2950-48	4	16	28	Yes
v101_L1_1u_2310_24	1	2950-24	1	23	0	Yes
v101_L1_1u_4710	1	2950-48	1	47	0	Yes
v101_L1_2u_2210_24	1	2950-24	2	22	0	Yes
<b>Cisco 2955</b>						
1u_710_2955	1 and 2	2955C-12	1	7	4	No
L1_1u_2955	1	2955C-12	1	11	0	No
L1_2u_2955	1	2955C-12	2	10	0	No
v101_1u_710_2955	1 and 2	2955C-12	1	7	4	Yes
v101_L1_1u_2955	1	2955C-12	1	11	0	Yes
v101_L1_2u_2955	1	2955C-12	2	10	0	Yes
<b>Cisco 2960/2960+</b>						
2u_1010_split_2960_24	1 and 2*	2960-24	2	10	10	No
2u_2960	2	2960-48	2	0	46	No
2u_2960_24	2	2960-24	2	0	22	No
4u_410_2960	2	2960-48	4	4	40	No
4u_410_2960_24	1 and 2	2960-24	4	4	16	No
4u_810_24	1 and 2	2950-24	4	8	12	No
4u_810_2960_24	1 and 2	2960-24	4	8	12	No
4u_1610_24	1 and 2	2960-24	4	16	4	No
4u_1610_2960_24	1 and 2	2960-24	4	16	4	No
4u_2110_split_2960	1 and 2*	2960-48	4	21	21	No
4u_2960	2	2960-48	4	0	44	No
4u_2960_24	2	2960-24	4	0	20	No
12u_2960_24	2	2960-24	12	0	12	No
24u_2960	2	2960-48	24	0	24	No
hmtf_2960_24	2	2960-24	24 HMTF Uplinks	0	0	No
L1_1u_2310_2960_24	1	2960-24	1	23	0	No
L1_1u_4710_2960	1	2960-48	1	47	0	No
L1_2u_2210_2960_24	1	2960-24	2	22	0	No
owv_mst_1u_2960_24	2	2960-24	24 OneWireless Uplinks	0	0	No

File name	Level	Switch type	Number of uplinks	Number of 10 MB FTEBs	Number. of FD 100 MBs	VLAN101 configured
owv_pvst_1u_2960_24	2	2960-24	24 OneWireless Uplinks	0	0	No
v101_2u_1010_2960_24	1 and 2*	2960-24	2	10	10	Yes
V101_2u_2960	2	2960-48	2	0	46	Yes
V101_2u_2960_24	2	2960-24	2	0	22	Yes
V101_4u_410_2960	1 and 2	2960-48	4	4	40	Yes
V101_4u_410_2960_24	1 and 2	2960-24	4	4	16	Yes
V101_4u_810_2960	1 and 2	2960-48	4	8	36	Yes
V101_4u_810_2960_24	1 and 2	2960-24	4	8	12	Yes
V101_4u_1610_2960_24	1 and 2	2960-24	4	16	4	Yes
V101-4u_2110_2960	1 and 2*	2960-48	4	21	20	Yes
V101_4u_2960_24	2	2960-24	4	0	20	Yes
V101_12u_2960_24	2	2960-24	12	0	12	Yes
V101_24u_2960	2	2960-48	24	0	24	Yes
V101_4u_1610_2960_0	1 and 2	2960-48	4	16	28	Yes
V101_4u_2960	2	2960-48	4	0	44	Yes
V101_L1_1u_2310_2960_24	1	2960-24	1	23	0	Yes
v101_L1_1u_4710_2960	1	2960-48	1	47	0	Yes
v101_L1_2u_2210_24	1	2950-24	2	22	0	Yes
<b>Cisco 3550</b>						
24u_3550fx	L2	3550-24	24	0	0	No
fte_3550_cnfg	L2	3550-12	12	0	0	No
v101_24u_3550fx	L2	3550-24	12	0	0	Yes
v101_fte_3550_cnfg	L2	3550-12	12	0	0	Yes
<b>Cisco 3560/V2</b>						
2u_1010_split_3560_24	1 and 2	3560-24	2	10	12	No
2u_3560_24	2	3560-24	2	0	22	No
4u_3560_24	2	3560-24	4	0	20	No
12u_3560_24	2	3560-24	12	0	12	No
V101_2u_1010_3560_24	1 and 2	3560-24	2	10	12	Yes
V101_2u_3560_24	2	3560-24	2	0	22	Yes
V101_4u_3560_24	2	3560-24	4	0	20	Yes
v101_12u_3560_24	2	3560-24	12	0	12	Yes

File name	Level	Switch type	Number of uplinks	Number of 10 MB FTEBs	Number. of FD 100 MBs	VLAN101 configured
<b>Cisco 3750</b>						
Fte_3750_cnfg	2	3750-12	12	0	0	No
V101_fte_3750_cnfg	2	3750-12	12	0	0	Yes
v101_stack1	2	3750-24 (up to 9)	0	0	0	Yes
<b>Cisco 3750x</b>						
Fte_3750x_cnfg	2	3750x-12	12	0	0	No
V101_fte_3750x_cnfg	2	3750x-12	12	0	0	Yes
v101_stack1	2	3750x-24 (up to 9)	0	0	0	Yes
3750x_Plugin	2	1 GB plug-in Module	4	0	0	0
<b>Cisco ie3000</b>						
8base_8expansion_ie3000_split*	1 and 2	8 port Base and 8 port Expansion	Gigabit only	7	7	No
L1_base_ie3000_4	1	4 port Base Unit	Gigabit only	4	0	No
L1_base_ie3000_8	1	8 port Base Unit	Gigabit only	8	0	No
L1_expansion_ie3000_8	1	8 port Expansion	0	8	0	No
L1_expansion_ie3000_16	1	Two 8 port Expansions	0	16	0	No
L2_base_ie3000_4	2	4 port Base Unit	Gigabit only	0	4	No
L2_base_ie3000_8	2	8 port Base Unit	Gigabit only	0	8	No
L2_expansion_ie3000_8	2	8 port expansion	0	0	8	No
L2_expansion_ie3000_8copper_8fiber	2	8 port copper and 8 port fiber expansion	0	0	16	No
L2_expansion_ie3000_8fibe	2	8 port fiber expansion	0	0	8	No
L2_expansion_ie3000_16	2	2 8 port expansion	0	0	16	No
v101_8base_8expansion_ie3000_split*	1 and 2	8 port Base and 8 port Expansion	Gigabit only	7	7	Yes
V101_l1_base_ie3000_4	1	4 port Base Unit	Gigabit only	4	0	Yes
V101_l1_base_ie3000_8	1	8 port Base Unit	Gigabit only	8	0	Yes

File name	Level	Switch type	Number of uplinks	Number of 10 MB FTEBs	Number. of FD 100 MBs	VLAN101 configured
V101_l1_expansion_ie3000_8	1	8 port expansion	0	8	0	Yes
v101_l1_expansion_ie3000_16	1	2 8 port expansions	0	16	0	Yes
V101_l2_base_ie3000_4	2	4 port Base Unit	Gigabit only	0	4	Yes
V101_l2_base_ie3000_8	2	8 port Base Unit	Gigabit only	0	8	Yes
V101_l2_expansion_ie3000_8	2	8 port expansion	0	0	8	Yes
v101_l2_expansion_ie3000_8copper_8fiber	2	8 port copper and 8 port fiber expansion	0	0	16	Yes
v101_l2_expansion_ie3000_8fiber	2	8 port fiber expansion	0	0	8	Yes
v101_l2_expansion_ie3000_16	2	2 8 port expansions	0	0	16	Yes
<b>Cisco 2960X</b>						
2u_2960x_24	2	2960X-24	2	0	22	No
4u_2960x_24	2	2960X-24	4		20	No
12u_2960X_24	2	2960X-24	12	0	12	No
v101_2u_2960x_24	2	2960X-24	2	0	22	Yes
v101_4u_2960x_24	2	2960X-24	4		20	Yes
v101_12u_2960x_24	2	2960X-24	12	0	12	Yes
vm_2u_2960x_24	2	2960X-24 1 GB Config	2	0	22	No
vm_4u_2960x_24	2	2960X-24 1 GB Config	4		20	No
vm_12u_2960X_24	2	2960X-24 1 GB Config	12	0	12	No
vm_v101_2u_2960x_24	2	2960X-24 1 GB Config	2	0	22	Yes
vm_v101_4u_2960x_24	2	2960X-24 1 GB Config	4		20	Yes
vm_v101_12u_2960x_24	2	2960X-24 1 GB Config	12	0	12	Yes

**Attention**

- \* These are split configurations. These are preferred for level1/2 combinations. 2 interfaces are lost to the L1/L2 crossover in the switch.
- This file must be modified for each switch in the stack. See “Modifying the stacked switch configuration files” on page 90 for details.
- IE300 switches are loaded with an image with the “base” characteristic in the file name. Additional ports are desired expansion modules which can be added to the base switch. After loading a “base” configuration a configuration with the “expansion” characteristic in the file name can also be loaded. The two split configurations are an exception. They are configured to have an 8 port base module and an 8 port copper expansion module. The “expansion” configuration files cannot be applied to the split switch configurations without modification.
- When using a vlan other than vlan 1 in your switch configurations you may see an SNMP event that an interface with an interface number greater than the number of ports on a switch has gone down when vlan 1 is shut down by the configuration.
- The 2960X switch uplinks are configured for 1GB uplink connections in all switch configurations.
- The SFP ports are not counted in the uplink port count, but are by default configured as uplink ports.



## 9.7 Configuring Cisco switches

Use the procedures in this section to install the switch configuration files to the node, and configure the Cisco switches for FTE using the command line interface of the switch and the correct switch startup configuration file.

You can also configure the Cisco switches and load files to a switch using the *Switch Configuration Tool*. The Switch Configuration Tool is developed by Honeywell and is available from Experion R430 and higher release. You can use the Switch Configuration Tool, which is pre-installed and ready to use in Experion PKS R430 and higher release for performing the following:

- Configuring Honeywell-qualified Cisco switches
- Creating and generating switch configuration files
- Loading the switch configuration files into Honeywell-qualified Cisco switches

Refer to the *Switch Configuration Tool User's Guide* for information about configuring a switch and loading files to a switch.

### Related topics

“Before you begin” on page 89

“Passwords and names for switch access and configuration” on page 89

“Tasks for configuring a Cisco switch” on page 90

“Accessing switch configuration files” on page 90

“Connecting locally to the switch” on page 91

“Configuring switch interface options” on page 92

“Using VLAN101 switch configuration files” on page 98

“Loading the switch configuration file” on page 98

### 9.7.1 Before you begin

Before beginning the procedures in this section, ensure that you verify the following:

- You have an RS-232 cable configured, as required by the switch vendor, to connect the computer's serial port to the switch's communication port.
- Verify or install the Tera Term package from the Experion PKS Installation media.
- You have reviewed the specific vendor's switch user guide, if necessary.

### 9.7.2 Passwords and names for switch access and configuration

During the switch configuration process, you are prompted for names and passwords. The following table lists the names and passwords used while configuring switches.

Name	Description	Examples used in this document
Virtual Terminal Password	Password used for protecting access to the router over a network interface.	FTE4
FTP Server Username	FTP server user name that allows you to use Telnet and FTP sessions to save and restore configuration options.	ps_user
FTP Server Password	FTP server password that allows you to use Telnet and FTP sessions to save and restore configuration options.	ps_user_local
Host Name	Host name for switch used for FTE.	Cisco_FTE4

Name	Description	Examples used in this document
Enable Secret	Password used for protecting access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.	Cisco_FTE1
Enable Password	Password used when you do not specify an enable secret password, with some older software versions, and some boot images.	FTE4

### 9.7.3 Tasks for configuring a Cisco switch

The following table lists the tasks for configuring the Cisco switches in an FTE network.

- Connect to the switch. Refer to “Connecting locally to the switch” on page 91.
- Verify the switches have the IOS version qualified by Honeywell as listed in the PDF on the Honeywell Process Solutions website (<http://www.honeywellprocess.com/library/support/software-downloads/Customer/FTE-Qualified-IOS-Firmware-for-Cisco-Switches.pdf>).



#### Attention

If the version is not the same as that listed in the document *FTE-Qualified-IOS-Firmware-for-Cisco-Switches.pdf*, contact Honeywell Network Services for the procedure to upgrade the IOS.

- Configure the switch. Refer to “Configuring switch interface options” on page 92.
- Load the switch configuration file. Refer to “Loading the switch configuration file” on page 98.

### 9.7.4 Accessing switch configuration files

Switch configuration files are packaged with the FTE driver and are copied to the following location when you run the FTE driver installation package.

- C:\Program Files\Honeywell\FTEDriver\Switch Configuration\cisco catalyst 2950
- C:\Program Files\Honeywell\FTEDriver\Switch Configuration\cisco catalyst 2955
- C:\Program Files\Honeywell\FTEDriver\Switch Configuration\cisco catalyst 2960
- C:\Program Files\Honeywell\FTEDriver\Switch Configuration\cisco catalyst 2960X
- C:\Program Files\Honeywell\FTEDriver\Switch Configuration\cisco catalyst 3550
- C:\Program Files\Honeywell\FTEDriver\Switch Configuration\cisco catalyst 3560
- C:\Program Files\Honeywell\FTEDriver\Switch Configuration\cisco catalyst 3750
- C:\Program Files\Honeywell\FTEDriver\Switch Configuration\cisco catalyst 3750X
- C:\Program Files\Honeywell\FTEDriver\Switch Configuration\Cisco ie3000

If you have not installed FTE, access the switch configuration files from the Experion PKS Installation media at the *Media Drive:\FTEDriver\Switch Configuration* location.

After connecting to the switch, use the switch’s command line interface (CLI) to configure the switch options. If the switch does not respond, press Enter and wait for the prompt (>) to appear.

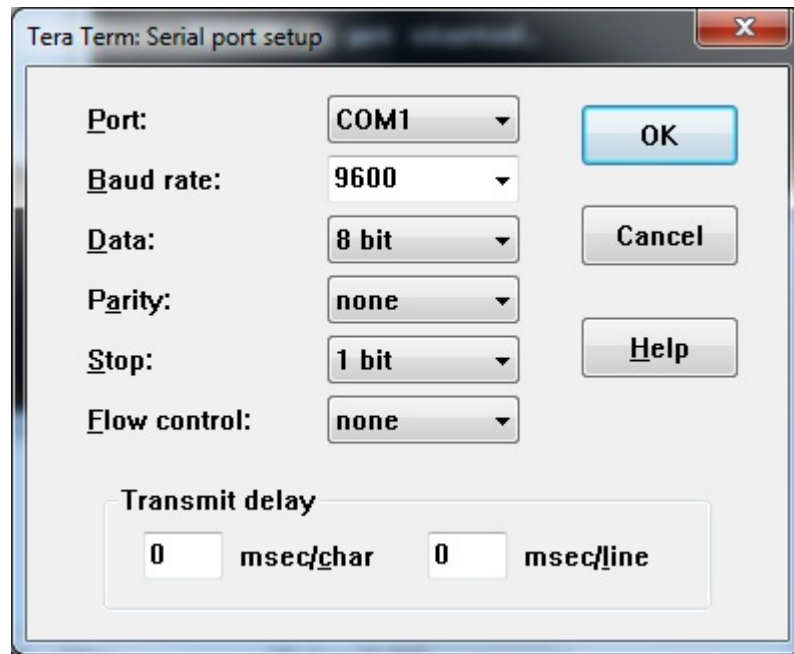
The following image lists the conventions used in the switch configuration procedures and examples.

At any point you may enter a question mark '?' for help. Use ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'.	Terminal sessions and system displays are shaded in gray and appear in a screen font.
Cisco_FTE4# <b>config t</b> Enter configuration commands, one per line. End with CNTL/Z. Cisco_FTE4(config)# <b>int vlan1</b>	Values that are entered by the user are in <b>bold</b> .
Enter host name [Switch]: <i>Cisco_FTE4</i>	Arguments for which the user supplies the values are in <b>bold italic</b> .
Destination filename [config.text]?<ENTER> Writing config.text !!!!	Nonprinting characters, such as passwords or Enter key, are in angle brackets (<>).

### 9.7.5 Connecting locally to the switch

Perform the following procedure to connect to the switch using a serial connection.

1. Connect the RS-232 cable to the switch's communication port and the computer's serial port.
2. Start a serial connection using the Switch Configuration Tool. (Refer to the *Establishing a serial connection using the Switch Configuration Tool* section in the *Switch Configuration Tool Users Guide*).
3. Start a Tera Term session with a serial connection. Tera Term can be installed from the Experion PKS Installation media by executing the installation package located at `\packages\Tera Term\teraterm_4.82.exe`.
  - Select All Programs> Term Term> Tera Term.
  - Select Setup>Serial port from the Tera Term Window. For more details on how to operate Tera Term Select Help>Index for details.



- Verify or configure the serial port settings:
    - Port: (Select COM port COM1 or COM2)
    - Bits per second: 9600
    - Data bits: 8 bit
    - Parity: none
    - Stop bits: 1 bit
    - Flow control: none
  - Click OK.
4. Power up the switch and go to the next procedure.

**! Attention**

- Do not power up the switch until instructed to do so.

### 9.7.6 Configuring switch interface options

Use the following procedure to enable the configuration dialog and basic management setup in the switch. After configuring the switch options, use the rest of the procedure to setup the switch IP address, enable SNMP traps, and establish the SNMP RO community and the NTP time service. Establishing an IP address allows you to use Telnet and FTP sessions to save and restore configuration options.



**Tip**

All values to be entered by the user appear in bold. Press ENTER after entering each value.

1. When the following display appears, type all values that appear in bold. Enter values for the text that appears in *bold italic*.

```

Would you like to enter the initial configuration dialog?
[yes/no]: y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: y
Configuring global parameters:

```

2. The host name is unique for each switch. The following are used as the examples in the switch displays.

- *Cisco\_FTE4*: example host name
- *Cisco\_FTE1*: example enable secret
- *FTE4*: example virtual terminal password
- *FTE4*: example enable password

Enter the host name and password when prompted.

3. When the following display appears, type all values that appear in **bold**. Specify your own values for the text that appears in **bold italic**.

```

Enter host name [Switch]: Cisco_FTE4

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret: Cisco_FTE1

The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password: FTE4

The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: FTE4
Configure SNMP Network Management? [no]: N

```

4. The following is an abridged example of what appears after the configuration. Press the SPACE BAR to advance the display when it pauses.

```

Current interface summary

Any interface listed with OK? value "NO" does not have a valid
configuration

Interface          IP-Address  OK?  Method  Status
Protocol
Vlan1              unassigned  NO   unset   up
down
FastEthernet0/1    unassigned  YES  unset   down
down
FastEthernet0/2    unassigned  YES  unset   down
down
FastEthernet0/3    unassigned  YES  unset   down
down
FastEthernet0/48   unassigned  YES  unset   down
down
GigabitEthernet0   unassigned  YES  unset   down
down
GigabitEthernet0/2 unassigned  YES  unset   down
down

```

5. After the configuration display is complete, the switch dialog appears. Type all values that appear in **bold**.

```

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
  Configure IP on this interface? [yes/no]: N
  Would you like to enable as a cluster command switch? [yes/no]: N

```

6. The following is an abridged example of what displays after the VLAN1 configuration.  
Press the SPACE BAR to advance the display when it pauses.

The following configuration command script was created:

```
hostname Cisco_FTE4
enable secret 5 $1$qF.3$3Aikt0lNtdjMLAdknUnht.
enable password FTE4
line vty 0 15
password FTE4
no snmp-server
!
!
interface Vlan1
shutdown
no ip address
!
interface FastEthernet0/1
no shutdown
no ip address
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4

interface FastEthernet0/48
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
end
```

7. After the configuration display is complete, the following switch dialog appears. Type **2** and press ENTER to save the switch configuration.

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
```

Enter your selection [2]: 2

8. The following display appears. This completes the switch configuration dialog. Complete the rest of the procedure to setup IP addressing, SNMP traps and the NTP time service for the switch.

```
Building configuration...
[OK]
00:02:36: %LINK-5-CHANGED: Interface Vlan1, changed state to
administratively down
00:02:37: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to down
00:02:38: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
Use the enabled mode 'configure' command to modify this
configuration.
```

**Attention**

The steps 9 through step 21 describes the manual tasks for setting up IP address, SNMP traps and the NTP time service for the switch. You can use the Switch Configuration Tool for performing these tasks.

9. Use the enable command and the enable secret previously established. *Cisco\_FTE1* is used in the following example. Type all values that appear in **bold**. Specify your values for the text that appears in ***bold italic***.

```
Press RETURN to get started!<ENTER>

Cisco_FTE4>enable

Password:Cisco_FTE1

Cisco_FTE4#config t

enter configuration commands, one per line. End with
CNTL/Z.
```

10. If VLAN 101 is to be used, initialize VLAN 101 by performing these additional steps.

- a. Type `vlan 101`
- b. Type `exit`

Otherwise, go to the next step.

11. To enable Telnet and FTP, use one of the following commands.

- To configure VLAN1, type **`int vlan1`**
- To configure VLAN101, type **`int vlan101`**

Type all values that appear in **bold**. Specify your own values for the text that appears in ***bold italic***.

```
Cisco_FTE4(config)#int vlan1
```

12. The following is used for the IP address and subnet mask in the following switch displays

10.1.4.253 255.255.255.0

Type all values that appear in **bold**. Specify your own values for the text that appears in ***bold italic***.

```
Cisco_FTE4(config-if)#ip address 10.1.4.253 255.255.255.0
Cisco_FTE4(config-if)#no shutdown
Cisco_FTE4(config-if)#exit
```

**Attention**

One of the nodes on the network must be set up as the FTP server. The FTP server requires a user name and a password that are registered in that machine with permissions to allow FTP access. You can then archive and restore configurations using Telnet and the FTP server.

13. A user name and password are required for the FTP server. The following are used as the examples in the switch displays. These commands can be added to the banner text using the switch configuration tool.

- *ps\_user* - example user name
- *ps\_user local* – example password
- *FTE4* – example virtual terminal password

Type all values that appear in **bold**. Specify your own values for the text that appears in ***bold italic***.



```
Cisco_FTE4(config)#ip ftp username ps_user
Cisco_FTE4(config)#ip ftp password ps_user local
```

14. The switch generates SNMP traps when the switch reboots or has a link go up or link go down. The switch must have a target IP address for the SNMP traps, which is the IP address of the server running the Experion system. Systems with redundant servers must have both server IP addresses configured in the switches for SNMP. You must also establish a community name for the switch.

The following are used as the examples in the switch displays.

- 10.1.4.15 - Experion server IP address
- FTE - Switch community name

Type all values that appear in **bold**. Specify your own values for the text that appears in ***bold italic***.

```
Cisco_FTE4(config)#snmp-server enable traps snmp warmstart
linkdown linkup coldstart
Cisco_FTE4(config)#snmp-server host 10.1.4.15 FTE snmp
```

15. If the system has redundant servers, repeat the following command using the redundant server IP address (10.1.4.16 – is used as an example for the redundant server IP address).

```
#snmp-server host 10.1.4.16 FTE snmp
```

16. To enable SNMP reads of the switch statistics, type the following command.

```
Snmp-server community public RO
```

**Public** is the community name default as configured in the Experion SPS. This is not a secure name and must have already been changed using the System Definition tool from Configuration Studio.



#### Attention

The Windows SNTP service does not provide the proper protocol for NTP that the switch requires. Hence, you must configure an NTP timeserver to synchronize time with other switches and network nodes. Examples of NTP Time servers are as follows:

- Router
- Dedicated NTP server node
- GPS based NTP server

If the NTP server is outside the FTE subnet, you must establish a default gateway.

17. The following are used as examples in the switch displays.

- 10.1.4.1 - Default gateway IP address
- 192.168.100.1 - NTP time server IP address

If the timeserver is within the FTE subnet, go to the next step. Otherwise, type all values that appear in **bold**. Specify your own values for the text that appears in ***bold italic***.

```
Cisco_FTE4(config)#ip default-gateway 10.1.4.1
```

18. Configure the NTP timeserver.

Type all values that appear in **bold**. Specify your own values for the text that appears in ***bold italic***.

```
Cisco_FTE4(config)#ntp server 192.168.100.1
```

19. If you are not using a stacked switch configuration, go to the next step. The following are used as examples in the switch displays.

- gig(2)/0/1 – 12 – (2) is the level of the switch in the stack
- (vlan 101) – VLAN1 is optional and must be the VLAN used if it is different from 101

Type all values that appear in **bold**. Specify your own values for the text that appears in ***bold italic***.

```
Cisco_FTE4(config)#int range gig(2)/0/1 - 12
Cisco_FTE4(config)#switchport access (vlan 101)
Cisco_FTE4(config)#switchport mode access
Cisco_FTE4(config)#sevice-policy input oda-policy
Cisco_FTE4(config)#srr-queue bandwidth share 1 2 3 4
```

20. Type **exit** and type **write**. The switch configuration is complete.

```
Cisco_FTE4(config)#exit
Cisco_FTE4#
00:06:03: %SYS-5-CONFIG_I: Configured from console by console
<ENTER>
```

21. The switch option configuration is complete. You are now ready to download the appropriate switch configuration file.

### 9.7.7 Using VLAN101 switch configuration files

If the VLAN1 in the switches must be disabled, you must use the alternate switch configuration files that are preceded with *V101\_*. For example, instead of using *4u.text*, use the *v101\_4u.text* file. See Table 9-4 for a list of all switch configuration files. The files with interface options for the VLAN1 are replicated with each interface attached to VLAN101. If a VLAN number other than 101 is needed, use a text editor to modify the current V101 file and replace all occurrences of 101 with the alternate VLAN number.

### 9.7.8 Loading the switch configuration file

The following procedure uses the Xmodem file transfer utility of Tera Term to transfer the correct switch configuration file from the installation media to the switch. After downloading the switch configuration file, write the configuration back to the switch memory.

You must familiarize with the base configuration files and modify them as necessary before loading them. For example, 2960 configuration files contain the following lines in the gigabit port configuration.

```
!Uncomment the following two lines if using a 100FX SFP module on this interface (module must be
present at the time of configuration)
! media-type sfp
! duplex full
```

If you are planning to connect 100FX fiber to this particular port remove the '!' from the two lines below the instruction and insert the fiber SFP into the switch before loading the configuration. Press ENTER after typing each value.



#### Tip

If you are not familiar with Xmodem, read Tera Term's help and try a transfer before initiating the transfer in the switch. Read steps 1 through 6 in the following procedure before you begin. This process can also be performed using the Serial File Transfer function of the Switch Configuration Tool.

1. To determine the most appropriate switch configuration file for your system, review the table described in section "Details for switch configuration files" on page 83.
2. Initiate the transfer in the switch using the copy command. Type all values that appear in **bold**.

```
Cisco_FTE4#copy xmodem: system:running-config
Destination filename [running-config]?<ENTER>
```

3. Initiate the transfer in Tera Term and choose the appropriate switch configuration file.
  - a. From the Tera Term menu bar, select **File > Transfer > XMODEM > Send**.

- b. Select and navigate to the **Switch Configuration** folder in one of the following location.
  - C:\Program Files (x86)\Honeywell\FTEDriver\SwitchConfigurationFiles
  - Media Drive:\Packages\FTE\_Driver\SwitchConfigurationFiles
  - Location you saved the files
- c. Select 1K Radio button.
- d. Select the correct switch configuration file for your particular system and click **OPEN**.
4. If there is a problem during the transfer, error messages are displayed, fix the problem with the switch configuration file, retype the following command, and then press **ENTER**.

```
Cisco_FTE4#copy xmodem: system:running-config
```

5. Initiate the transfer in Tera Term by repeating step 3.
6. The following message appears when the transfer is complete.

```
16256 bytes copied in 46.396 secs (353 bytes/sec)
```

7. Write the basic switch configuration file and the switch configuration file you downloaded back to the switch memory by typing all values that appear in **bold**.

```
Cisco_FTE4#write
```

8. Display the new switch configuration options on the screen by typing all values that appear in **bold**.

```
Cisco_FTE4#sho run
```

9. The following abridged example of the switch display uses options based on the switch configuration file previously selected.
  - 4 uplink ports
  - 4 autospeed ports for FTEB
  - Remaining ports at 100 MB

Press the space bar to advance the display when it pauses.

```

Building configuration...

Current configuration : 15560 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service sequence-numbers
!
hostname Cisco FTE4
!
enable secret 5 $1$JIQ6$IJ3nKv2oS2zCJZihoHEK1/
enable password Cisco FTE1
!
wrr-queue bandwidth 1 2 3 4
!
class-map match-all cda_medium
  match access-group 104
class-map match-all cda_urgent
  match access-group 102
class-map match-all cda_high
  match access-group 103
class-map match-all cda_low
  match access-group 105
!
!
policy-map cda_policy
  class cda_urgent
    set ip dscp 56
  class cda_high
    set ip dscp 46
!
ip subnet-zero
ip ftp username ps_user
ip ftp password ps user local
no ip igmp snooping
!
spanning-tree extend system-id
!
!...

```

```

interface FastEthernet0/1
  no ip address
  duplex full
  speed 100
  service-policy input cda_policy
  storm-control broadcast level 20.00 18.00
  storm-control multicast level 20.00 18.00
  storm-control unicast level 20.00 18.00
  storm-control action trap
!
interface FastEthernet0/48
  switchport trunk allowed vlan 1,1001-1005
  no ip address
  duplex full
  speed 100
  service-policy input cda_policy
  storm-control broadcast level 20.00 18.00

  storm-control multicast level 20.00 18.00
  storm-control unicast level 20.00 18.00
  storm-control action trap
  spanning-tree portfast
!
interface GigabitEthernet0/1
  no ip address
  service-policy input cda_policy
  storm-control broadcast level 5.00 4.50
  storm-control multicast level 5.00 4.50
  storm-control unicast level 5.00 4.50
  storm-control action trap
!
interface GigabitEthernet0/2
  no ip address
  service-policy input cda_policy
  storm-control broadcast level 5.00 4.50
  storm-control multicast level 5.00 4.50
  storm-control unicast level 5.00 4.50
  storm-control action trap
!...

```

```

interface Vlan1
 ip address 10.1.4.254 255.255.255.0
 no ip route-cache
 shutdown
!
ip http server
!
access-list 102 permit tcp any any eq 55554
access-list 102 permit tcp any any eq 55555
access-list 103 permit tcp any any eq 55550
access-list 103 permit tcp any any eq 55551
access-list 103 permit tcp any any eq 55553
access-list 103 permit tcp any any eq 55552
access-list 103 permit tcp any any eq 55556
access-list 104 permit tcp any any eq 55557
access-list 104 permit tcp any any eq 55558
access-list 104 permit tcp any any eq 55559
access-list 104 permit udp any any eq 12321
access-list 104 permit tcp any any eq 55560
access-list 105 permit tcp any any eq 55560
access-list 105 permit udp any any eq 55560
access-list 105 permit tcp any any eq 55559
access-list 105 permit udp any any eq 12321
access-list 105 permit tcp any any eq 55556
access-list 105 permit tcp any any eq 55557
access-list 105 permit tcp any any eq 55558
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password FTE1
 login
line vty 5 15
 password FTE1
 login
!
end

Cisco_FTE4#

```

10. This completes the switch configuration. To archive the configuration file for future use, refer to section “Saving and modifying Cisco switch configuration files” on page 103.

## 9.8 Saving and modifying Cisco switch configuration files

Use the procedures in this section to save, modify and restore switch configuration files. Following are the circumstances where you must perform these tasks.

- A switch fails and you must reload the switch configuration file.
- Add a new node type to the network.
- Use an existing configuration file on another switch.

It is recommended that the Switch Configuration Tool be used for modifying and restoring the Cisco switch configuration files. Refer to the *Switch Configuration Tool Users Guide* for further information.

### Related topics

“Downloading the switch configuration file (optional)” on page 103

“Enabling Telnet on your system” on page 104

### 9.8.1 Downloading the switch configuration file (optional)

Use the following procedure to save a file containing the configured switch options. This helps in reconfiguring the switch in case of a switch failure. Press ENTER after entering each value.

1. Open a Telnet session from the command window on the FTE server node.
2. Click **Start > Run** and type **cmd** in the **Run** dialog box.
3. At the command prompt type telnet followed by the IP address set in the switch configuration. *10.1.4.253* is used in the following example.

```
cmd>telnet 10.1.4.253
```

4. If the switch connection is successful, you are prompted for a password. Type the virtual terminal password previously configured for the switch and press ENTER.

*FTE4* is used in the following example.

```
User Access Verification
Password:FTE4
```

5. The enable command and the enable secret you previously configured allow you to access the switch configuration file in order to copy it.

*Cisco\_FTE1* is used in the following example.

Type all values that appear in **bold**. Specify your own values for the text that appears in ***bold italic***.

```
Cisco_FTE4#enable
Password:Cisco FTE1
```

6. Use the copy flash command followed by the name of the switch configuration file and ftp command to copy the switch configuration file from flash memory.

```
Cisco_FTE4#copy flash:config.text ftp:
```

7. Enter IP address of the FTP server to copy the switch configuration file from the switch memory to the FTP server node.

*10.1.4.15* is used in the following example.

Supply your own values for the text that appears in ***bold italic***.

```

Address or name of remote host []?10.1.4.15
Destination filename [config.text]?<ENTER>
Writing config.text !!!!
15197 bytes copied in 4.240 secs (3799 bytes/sec)
Cisco_FTE4#

```

8. The switch configuration file is saved in the **inetpub\ftproot** directory on the ftp server. Rename the *config.text* file to the switch host name. This allows you to download all the switch configuration files to this location.

**Attention**

If several switches are configured at once, the ftp archiving can be done at the same time.

## 9.8.2 Enabling Telnet on your system

Perform the following procedure to enable Telnet on your system. Telnet is enabled by default on all Experion installed computers

1. Choose **Start > Settings > Control Panel**.

The **Control Panel** window appears.

2. In the left pane, click **Classic View**, and choose **Programs and Features**.

Or

In the left pane, click **Control Panel Home**, and choose **Programs > Programs and Features**.

3. Click **Turn Windows features on or off**.

The **User Account Control** dialog box appears.

4. Click **Continue**.

The **Windows Features** dialog box appears.

5. Check the following options.

- Telnet client
- Telnet server

6. Click **OK**.

The Telnet feature is now configured on your system.



## 9.9 Updating the Honeywell control firewall firmware

The Control Firewall Update Tool is an optional tool used to update the Control Firewall firmware revision. The tool, which is only available on FTE nodes, is launched from Configuration Studio or as a stand-alone application. If you try to launch the tool from a non-FTE node, an error message will be displayed.

### Related topics

- “Firewall devices” on page 105
- “Determining necessity of firmware update” on page 105
- “Firewall firmware update process” on page 105
- “Before using the control firewall update tool” on page 106
- “Launch the control firewall update tool” on page 106

### 9.9.1 Firewall devices

The firewall has the following two devices that require a firmware update. It is important that updates for both devices be performed at the same time.

- Control microprocessor
- Filter FPGA

### 9.9.2 Determining necessity of firmware update

Do not update the firmware image on the Honeywell control firewall until you have verified it is necessary by doing the following:

- Review the Software Change Notice (SCN) for your release to determine the required Honeywell control firewall firmware image for your release.
- Determine the current firmware revision by viewing the System Status detail display for the Honeywell control firewall.

### 9.9.3 Firewall firmware update process

#### Control microprocessor update

1. The new image is sent over the network in 256 byte chunks.
  - The firewall's 9th port LED flashes in a regular pattern.
  - Process takes approximately two minutes.
  - Once all the packets are sent, the image is checked for CRC-32 to ensure that there were no data errors.
  - When the process is complete, the 9th port LED stops flashing and returns to normal operation.
2. The CRC is calculated.
  - If there are nodes connected, the last two LEDs appear dim slightly.
  - If there are no nodes connected, the last two LEDs alternate blinking at a low intensity.
  - Process takes less than two minutes.
  - If the CRC is good, the new image is flashed into the microprocessor.
  - The 9th port LED flashes in a regular pattern.
3. After the new image is flashed into the microprocessor, the Honeywell control firewall is reset.
  - Process takes approximately one minute.
  - After the reset, the last two LEDs alternately flash.

- Approximately one minute after initialization, the update tool displays the new microprocessor revision.

#### **FPGA update**

1. The packets are sent over the network.
  - Process takes approximately four minutes.
  - The firewall's 9th port LED flashes in a regular pattern.
  - When the process is complete, the 9th port LED stops flashing and returns to normal operation.
2. The CRC-32 is calculated.
  - If there are nodes connected, the last two LEDs will dim slightly.
  - If there are no nodes connected, the last two LEDs will alternate blinking at a low intensity.
  - Process takes less than four minutes.
  - If the CRC-32 is successful, the Honeywell control firewall is reset.
3. The new image loads into the FPGA during the initialization after the reset.
  - The last two LEDs alternate flashing.
  - Approximately one minute after initialization, the update tool displays the new FPGA revision.

### **9.9.4 Before using the control firewall update tool**

Ensure that all of the following conditions are fulfilled before you can use this tool.

- The Control Firewall Update Tool package must be installed.
- The FTEMux driver must be installed and configured.
- The Honeywell Control Firewall must be added to the Network Tree within Configuration Studio.

If you can communicate with the Honeywell control firewall from the local node, the Control Firewall Update Tool appears as a task from the control firewall device.

### **9.9.5 Launch the control firewall update tool**

#### **To launch the tool from Configuration Studio**

1. Expand the network tree and click on devices.
2. From the right pane, select **Launch control firewall update tool**.
3. For more information, see the online help accessed from the tool.

#### **To launch the tool from the Start menu**

1. From your computer's Start menu, select **All Programs > Honeywell Experion PKS > Engineering Tools > Control Firewall Update**.
2. For more information, see the online help accessed from the tool.

# 10 Configuring a switch for SSH

## **Related topics**

“Configuring Cisco switch for SSH” on page 108

“Using Tera Term for SSH Communications” on page 110

## 10.1 Configuring Cisco switch for SSH

Configuring the Cisco switch for secure telnet or SSH connections enables passwords and connections to the switch to be encrypted, thereby making a secure communication, unlike plain text passwords are not sent over the Ethernet.



### Attention

- Ensure that the switch is configured using Experion Switch Configuration Files or FTE Switch tool before you begin configuring them for SSH.

### To verify crypto IOS

- Connect to the switch using the serial port “Connecting locally to the switch” on page 91 or using telnet connection.
- At switch> prompt: Type **enable** and enter password.
- At the switch# prompt type **show version**.

The output appears as follows: (for example the 2960+-48)

```
switch#sho version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE6, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled wed 09-Apr-14 03:40 by prod_rel_team

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 15.0(2r)EZ1, RELEASE SOFTWARE (fc1)
.
```

Switch Ports Model	SW Version	SW Image
* 1 50 WS-C2960+48TC-L	15.0 (2) SE6	C2960-LANBASEK9-M

- Verify that the software image contains the **K9** as shown in the **SW Image** column.
- If **switch# sho run** has the following output, it shows that crypto keys have been generated.

```
crypto pki trustpoint TP-self-signed-3164301184
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-3164301184
  revocation-check none

  rsakeypair TP-self-signed-3164301184
  !
  !
crypto pki certificate chain TP-self-signed-3164301184
certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  .
  .
  .
  38DD15D3 8775C117 4B497A0E 15D7D319 3C0CEF7E 1F34BEB5 0609126B 870737A8
  16D5FA5A 34D7B053 0F616533 F694AE55 39544F6D B7CAB347 6E6AE3D9 5A251606
  26B594E5 0507A92C 80FF605A B1501D
quit
```

- If both the above steps are not true, contact your technical support to update the switches IOS to support Crypto and SSH.
- Continue with **To setup SSH on the switch** when completed.

### To setup SSH on the switch

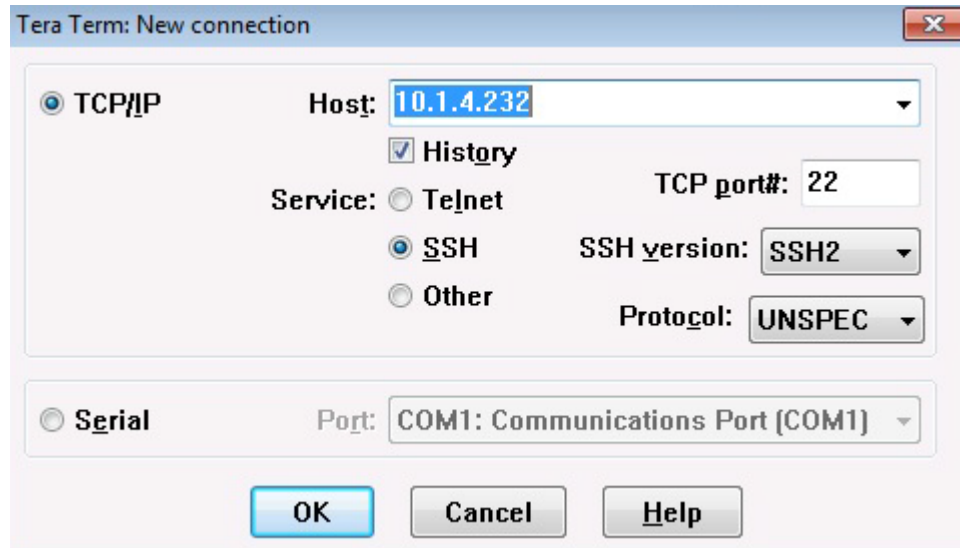
- Enter configuration mode: switch# **config t**
- If the above was true and Crypto keys already exist, and the ones already generated meet the sites standards, skip the next step.

- 3 Set the configuration, hostname and domain name for the switch This is used as a basis for the Keys.
  - a Switch(config)# **ip domain-name** <domain Name> (where >domain-name> is the domain name for the FTE community)
  - b Switch(config)# **crypto key generate rsa**  
  
 The name for the keys are: switchname.<domain-name> Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
  - c Number of bits in the modulus [512]: **1024**  
  
 % Generating 1024 bit RSA keys ...[OK]
- 4 Configure additional parameters for the SSH Connection. These values should be selected based on the site security policy.
  - a Switch(config)# **ip ssh authentication-retries 5**
  - b Switch(config)# **ip ssh time-out 120**
  - c **ip ssh version 2**
- 5 Set the username and password, and then configure the device to accept local authentication for the line vty connections.
  - a Switch(config)# **username** <UserName>**password**<Password>
  - b Switch(config)# **line vty 0 15**
  - c Switch(config-line)# **login local**
  - d Switch(config-line)# **end**
- 6 Configure verify SSH connection is setup correctly by going to Using Tera Term for SSH Communications.
- 7 If the connection was verified working, disable telnet, if required.
  - a Enter configuration mode: Switch# **config t**
  - b Switch(config)# **line vty 0 15**
  - c Switch(config-line)# Switch(config-line)# **transport input ssh**
  - d Switch(config-line)# **end**
- 8 Write the switch configuration.
  - a Enter configuration mode: Switch# **write memory**  
  
 Building configuration...  
 [OK]
- 9 Exit this session and use a SSH connection to connect to the switch and telnet connections are now disabled.

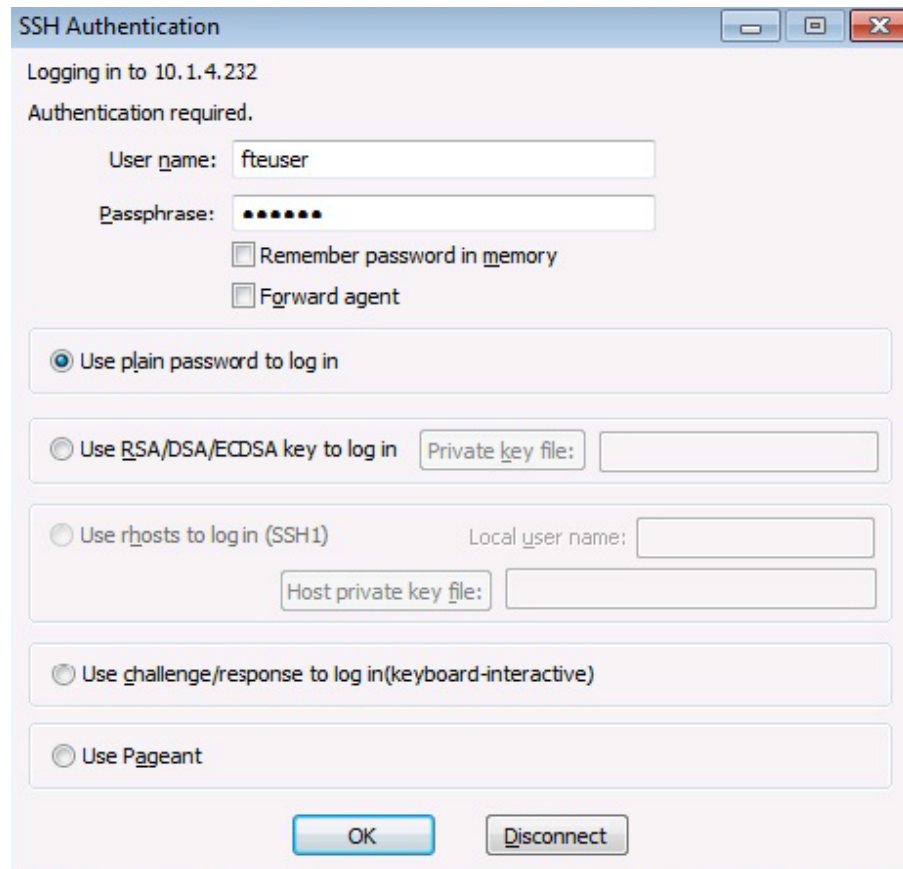
## 10.2 Using Tera Term for SSH Communications

Using Tera Term is the recommended connected way to have secure communications with the Cisco switches. This ensures that the passwords are encrypted and that monitoring of the network traffic do not reveal passwords as telnet does.

- 1 Install the Tera Term application from the Honeywell Experion PKS Installation DVD.
- 2 From the Start, click Menu **All Programs> Tera Term> Tera Term**  
Verify the Tera Term New Connection window.



- 3 Select **TCP/IP**.
- 4 In **Host** text Box: enter in the switches IP address, Select SSH Version as SSH2. Verify TCP Port# is **22**. Leave all other options as default.
- 5 Select **OK**. Verify **SSH Authentication** window.



SSH Authentication

Logging in to 10.1.4.232

Authentication required.

User name:

Passphrase:

☐ Remember password in memory

☐ Forward agent

☒ Use plain password to log in

☐ Use RSA/DSA/ECDSA key to log in Private key file:

☐ Use rhosts to log in (SSH1) Local user name:

Host private key file:

☐ Use challenge/response to log in(keyboard-interactive)

☐ Use Pageant

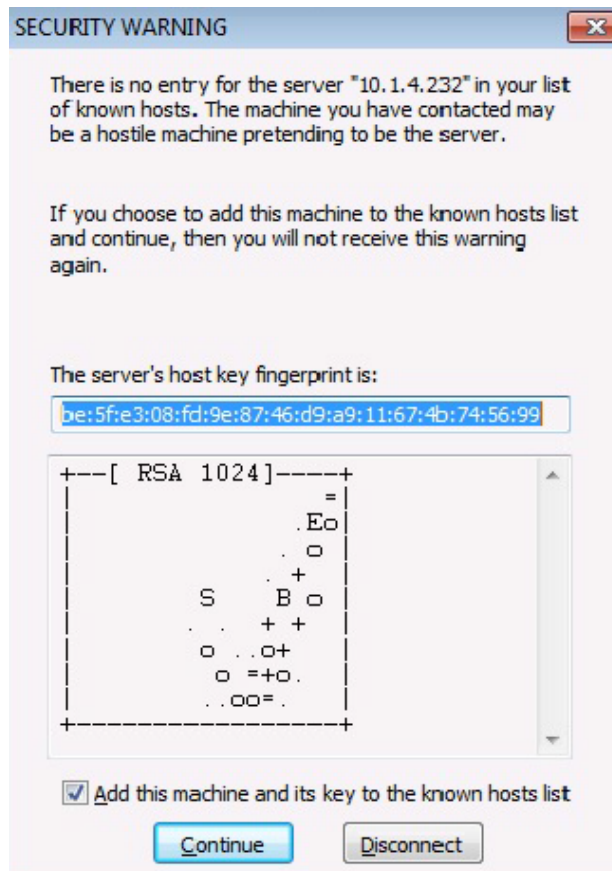
OK Disconnect

- 6 Verify the **Security Warning** window to add the key into the machine's known host list. Select **Continue**.



**Attention**

This window is prompted only once for each computer connection.



- 7 From SSH Authentication window: type in user <UserName> and passphrase: <Password>. If desired, uncheck **Remember Password in memory**, select **OK**.  
Where the <UserName> and <Password> are the User Name and Password entered in the previous section.
- 8 Verify Tera Term VT window with the switches prompt active, i.e., switch>. enter in enable, enter switch's secret password, verify switch#.



# 11 Troubleshooting Network Issues

## **Related topics**

“Preventing Crosslink Errors” on page 114

“Intermittent or blocked communication to controllers on a different subnet” on page 116

“Mismatch of FTE multicast address and destination port” on page 117

## 11.1 Preventing Crosslink Errors

### Related topics

“FTE diagnostic messages” on page 114

“Definition of crosslink error” on page 114

“Potential causes of crosslink errors” on page 114

### 11.1.1 FTE diagnostic messages

FTE sends diagnostic messages on each of the FTE interface ports. One part of the diagnostic message designates the interface port for the message. That is, whether the message is transmitted on the *Yellow* tree or on the *Green* tree. FTE uses the MAC address to define which interface is *Yellow* and which interface is *Green*. The interface port connection that has lower MAC address is defined as *Yellow* and the interface port connection that has higher MAC address is defined as *Green*. This binding order must remain consistent to maintain the correct interface port designation for the messages.

### 11.1.2 Definition of crosslink error

Both types of diagnostic messages (*yellow* and *green*) are transmitted on both FTE trees when the network has a switch crossover cable connected. However, when the trees are isolated from one another, the diagnostic messages must also be isolated. Only messages designated as *Yellow* must be seen on the *Yellow* tree and only messages designated as *Green* must be seen on the *Green* tree. A crosslink error occurs when, even after the crossover cable is removed and the trees are isolated, *Yellow* diagnostic messages are seen on the *Green* tree or green diagnostic messages are seen on the *Yellow* tree.

### 11.1.3 Potential causes of crosslink errors

The following table lists some of the causes for crosslink errors and gives examples how they occur.

Cause	Examples
Cables are crossed at the node or at the switches	<ul style="list-style-type: none"> <li>Cable with the <i>Yellow</i> boot is connected to the switch in the <i>Yellow</i> tree, but it is connected to the second port.</li> <li>Cable with the <i>Green</i> boot is connected to the switch in the <i>Green</i> tree, but it is connected to first port.</li> <li>Connection for first port (cable with <i>Yellow</i> boot) is connected to the switch in the <i>Green</i> tree.</li> <li>Connection for second port (cable with the <i>Green</i> boot) is connected to the switch in the <i>Yellow</i> tree.</li> </ul>
Both FTE cables are connected to the same tree	Cable with the <i>Yellow</i> boot and cable with the <i>Green</i> boot are connected to the same switch.
Binding order is “reversed”	<ul style="list-style-type: none"> <li>Cable with the <i>Yellow</i> boot is connected to the first port and to the Switch in the <i>Yellow</i> Tree, but the connection for the first port has higher MAC address.</li> <li>Cable with the <i>Green</i> boot is connected to the second port and to the Switch in the <i>Green</i> tree, but the connection for the second port has lower MAC address.</li> </ul>
FTE network topology does not follow configuration rules	<p>Any condition that creates network path loops, such as any of the following:</p> <ul style="list-style-type: none"> <li>FTE network has more than one crossover cable</li> <li>Multiple connections to an external network</li> <li>Switches are not in a tree hierarchy</li> </ul>

Cause	Examples
Several servers have multiple (4) NIC connections	Verify which cables are inserted

---

## 11.2 Intermittent or blocked communication to controllers on a different subnet

When Controllers are addressed in a different subnet than the server/console, the level 2 nodes rely on *addroute* and *ARP* to establish TCP connections with controllers. If proxy ARP is enabled on the router, the router responds with its own MAC address when the level 2 nodes ARP for the controller MAC addresses, preventing or breaking TCP communication. Hence, all router connections to an FTE network must have the *no ip proxy arp* command.

---

## 11.3 Mismatch of FTE multicast address and destination port

An FTE node does not show up in the FTE node list or FTE status display as expected.



# 12 Switch and Router Configuration Examples

## **Related topics**

“Cisco switch and router examples” on page 120

“Cisco router configuration statements” on page 121

“Subnet mask derivation” on page 123

“Stacked switch configuration examples” on page 124

---

## 12.1 Cisco switch and router examples

### **Cisco 2960 Configuration Example**

The following configuration file is an example of 4u\_410\_2960\_24.text which will configure.

- 4 uplinks (downlinks)
- 4 FTEB ports configured
- 40 100 Megabit or GBIC ports



## 12.2 Cisco router configuration statements

To configure the FTE community filtering requirements in Cisco routers, specific configuration commands are used, examples of which are provided in this section.

### Related topics

“Access control lists” on page 121

“Cisco 3560, 2960, IE3000 access list for protecting Safety Manager or third-party safety controllers” on page 122

### 12.2.1 Access control lists

Cisco uses an Access Control List (ACL) to describe what must pass and what must not pass through an interface. Following is an example of a set of ACLs used to provide the filtering.

```
access-list 101 permit tcp 10.0.0.0 0.0.0.255 any established
```

**Established connections are allowed in the whole FTE community subnet**

**The range of addresses in this FTE community is 10.0.0.2-255**

```
access-list 101 permit udp host 225.7.4.103 any
```

```
access-list 101 permit udp any host 225.7.4.103
```

**The DSA multicast address, 225.7.4.103 is allowed to pass in both directions**

```
access-list 101 permit ip 10.0.0.0 0.0.0.240 any
```

```
access-list 101 permit ip any 10.0.0.0 0.0.0.240
```

**The server range is 10.0.0.2-15**

```
access-list 101 permit udp any any eq domain
```

**Access to a domain controller TCP port is allowed.**

```
access-list 101 permit udp any any eq 88
```

**Access to a Kerberos server is allowed**

```
access-list 101 permit udp any any eq 389
```

**Access to a LDAP server is allowed**

**There is an assumed “deny all” at the end of the list. This means that any other address range is denied access.**

**These access lists are attached to the VLAN the FTE community is connected with as shown in the following example:**

```
interface Vlan101 ip address 10.0.0.1 255.255.255.0
```

**VLAN 101 is the FTE community VLAN. The FTE default gateway address is 10.0.0.1. The subnet mask of 255.255.255.0 will allow traffic in this range to pass to the ACL filters**

```
ip access-group 101 out
```

**Access-group 101 uses the ACLs described above in access-list 101**

```
no ip proxy-arp
```

**Proxy arp must be disallowed to enable hiding the L1 addresses from L3**

```
ip pim dense-mode
```

**PIM dense-mode is needed for the DSA multicasts to be routed.**

**The following is an example router interface configuration for the interface where the FTE community is connected.**

```
interface FastEthernet2/3
```

**This example has a connection to a 4006 interface in slot 2, third fast Ethernet port.**

```
switchport access vlan 101
```

```
switchport mode access
```

**The switchport (this interface) is set to be access to a VLAN and the VLAN is set to 101. The above ACLs were attached to VLAN 101**

```
duplex full
```

```
speed 100
```

**The speed and duplex if the interface is fixed to avoid problems with autosensing.**

### 12.2.2 Cisco 3560, 2960, IE3000 access list for protecting Safety Manager or third-party safety controllers

A level of protection is required for embedded nodes such as Safety Manager by limiting the nodes allowed onto the Safety Ethernet network to the servers that access the nodes. In this example, the servers have addresses 10.1.4.10 and 10.1.4.11. The protection consists of an access list to define the allowed addresses and an access group attached to the crosslink interface of the split switch on the L1 half. The configuration file contains the following:

- Access-list 130 permit ip 10.1.4.10 0.0.0.0 any
- Access-list 130 permit ip 10.1.4.11 0.0.0.0 any
- The standard configuration for the split switch file can be modified to substitute the above for the access-list 130 in the file before downloading to the switch
- Hence, for a split switch the L1 uplink interface is Fast Ethernet 0/13 so the configuration file contains the following:
  - interface FastEthernet0/13
  - switchport access vlan 1
  - switchport mode access
  - no ip address
  - duplex full
  - speed 100
  - ip access-group 130 in

The multicast and broadcast storm control on this interface are not needed due to the strict filtering, only allowing server traffic through.

---

## 12.3 Subnet mask derivation

For connected networks, three subnet masks must be derived from the number of supported nodes. Some number of least significant bits of the netmask must be set to zero to cover the number of nodes on the subnet (from each node's point of view).

### L2-L3 router port netmask example

- Two server FTE nodes = 4 IP Addresses
- Gateway (router port) = 1 IP Address
- $4 + 1$  rounded up to power of 2 = 8, or 0xFFFFFF8 (255.255.255.248)

### L2 node netmask example

- Sixteen non-server FTE nodes = 32 IP Addresses
- $4 + 1 + 32$  rounded up to power of 2 = 64 or 0xFFFFFC0 (255.255.255.192)

### Route add mask example

- Number of embedded FTE nodes \* 2 rounded up to power of 2
- Max FTE nodes is 511 = 1024 or 0xFFFFC00 (255.255.252.0)
- L1 Node Netmask
- Must ignore all unique L2 and L1 address bits = 0xFF000000 = 255.0.0.0

---

## 12.4 Stacked switch configuration examples

### Related topics

“Single domain controller with a 100 mb or CF9 connection” on page 124

“Uplink to 100 mb switch connection on switch 1, port 12” on page 124

### 12.4.1 Single domain controller with a 100 mb or CF9 connection

Following is an example of a stacked switch configure file that configures the second switch in the stack with a 100 mb connection on port 12 to be used for a CF9 or single domain controller connection.

```
interface GigabitEthernet2/0/12
  switchport access vlan 101
  switchport mode access
  service-policy input cda_policy
  speed 100
  duplex full
  srr-queue bandwidth share 1 2 3 4
  spanning-tree portfast
```

### 12.4.2 Uplink to 100 mb switch connection on switch 1, port 12

Following is an example of a stacked switch configuration file that configures the first switch in the stack with a 100 mb uplink connection on port 12.

```
interface GigabitEthernet1/0/12
  switchport access vlan 101
  switchport mode access
  service-policy input cda_policy
  speed 100
  duplex full
  srr-queue bandwidth share 1 2 3 4
```

# 13 Notices

## **Trademarks**

Experion®, PlantScape®, SafeBrowse®, TotalPlant®, and TDC 3000® are registered trademarks of Honeywell International, Inc.

OneWireless™ is a trademark of Honeywell International, Inc.

## **Other trademarks**

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

## **Third-party licenses**

This product may contain or be derived from materials, including software, of third parties. The third party materials may be subject to licenses, notices, restrictions and obligations imposed by the licensor. The licenses, notices, restrictions and obligations, if any, may be found in the materials accompanying the product, in the documents or files accompanying such third party materials, in a file named third\_party\_licenses on the media containing the product, or at <http://www.honeywell.com/ps/thirdpartylicenses>.

---

## 13.1 Documentation feedback

You can find the most up-to-date documents on the Honeywell Process Solutions support website at:

<http://www.honeywellprocess.com/support>

If you have comments about Honeywell Process Solutions documentation, send your feedback to:

[hpsdocs@honeywell.com](mailto:hpsdocs@honeywell.com)

Use this email address to provide feedback, or to report errors and omissions in the documentation. For immediate help with a technical problem, contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.

---

## 13.2 How to report a security vulnerability

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software.

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.

To report a potential security vulnerability against any Honeywell product, please follow the instructions at:

<https://honeywell.com/pages/vulnerabilityreporting.aspx>

Submit the requested information to Honeywell using one of the following methods:

- Send an email to [security@honeywell.com](mailto:security@honeywell.com).
- or
- Contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.

---

## 13.3 Support

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC). To find your local CCC visit the website, <https://www.honeywellprocess.com/en-US/contact-us/customer-support-contacts/Pages/default.aspx>.



---

## 13.4 Training classes

Honeywell holds technical training classes on Experion PKS. These classes are taught by experts in the field of process control systems. For more information about these classes, contact your Honeywell representative, or see <http://www.automationcollege.com>.

