Honeywell

Experion

Fault Tolerant Ethernet Overview & Implementation

Guide

EP-DSX244
R301
12/2006

R301

Notices and Trademarks

Honeywell International

Process Solutions

2500 West Union Hills

Phoenix, AZ 85027

1-800 343-0228

About This Document

This document provides an overview of Honeywell's Fault Tolerant Ethernet (FTE) and detailed network planning information.

Release Information

Document Name	Document ID	Release Number	Publication Date
Fault Tolerant Ethernet Fault Tolerant Ethernet Overview & Implementation Guide - **FE02**	EP-DSX244	R301	12/2006

References

The following list identifies all documents that may be sources of reference for material discussed in this publication.

Document Title
Fault Tolerant Ethernet Specification and Technical Data
Fault Tolerant Ethernet Installation and Service Guide
TPS Users
TPS System Implementation Guide for Windows 2000
TPS System Planning Guide for Windows 2000
TPS System Administration Guide for Windows 2000
Experion PKS Users
Experion PKS Overview
Experion PKS Software Installation and Upgrade Guide
Server and Client Planning Guide
Server and Client Configuration Guide (for Experion PKS)
Experion PKS Operators Guide

Contacts

World Wide Web

The following Honeywell web sites may be of interest to Process Solutions customers.

Honeywell Organization	WWW Address (URL)
Corporate	*http://www.honeywell.com*
Process Solutions	*http://www.acs.honeywell.com*
International	*http://content.honeywell.com/global/*

Telephone

Contact us by telephone at the numbers listed below.

	Organization	Phone Number	
United States and Canada	Honeywell International Inc. Industry Solutions	1-800-343-0228 1-800-525-7439 1-800-822-7673	Sales Service Technical Support
Asia Pacific	Honeywell Asia Pacific Inc. Hong Kong	(852) 23 31 9133	
Europe	Honeywell PACE Brussels, Belgium	[32-2] 728-2711	
Latin America	Honeywell International Inc. Sunrise, Florida U.S.A.	(954) 845-2600	

Symbol Definitions

The following table lists those symbols used in this document to denote certain conditions.

Symbol	Definition
	**ATTENTION:** Identifies information that requires special consideration.
	**TIP:** Identifies advice or hints for the user, often in terms of performing a task.
	**REFERENCE -EXTERNAL:** Identifies an additional source of information outside of the bookset.
	**REFERENCE - INTERNAL:** Identifies an additional source of information within the bookset.
CAUTION	Indicates a situation which, if not avoided, may result in equipment or work (data) on the system being damaged or lost, or may result in the inability to properly operate the process.
	**CAUTION**: Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury. It may also be used to alert against unsafe practices. **CAUTION** symbol on the equipment refers the user to the product manual for additional information. The symbol appears next to required information in the manual.
	**WARNING**: Indicates a potentially hazardous situation which, if not avoided, could result in serious injury or death. **WARNING** symbol on the equipment refers the user to the product manual for additional information. The symbol appears next to required information in the manual.

Contents

Tables

Figures

1. Introduction

1.1 About this guide

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. It is also assumed that any person performing an FTE network installation is familiar with networking fundamentals. Table 1-3 contains a list of useful documents from third-party vendors.

Typical users of this document

Typical users of this guide would include:

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

Acronyms and abbreviations

The following acronyms are associated with FTE and used throughout this guide.

Table 1-1 FTE 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 PKS
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
PIN	Plant Information Network
STP	Shielded Twisted Pair
TCP	Transport Control Protocol
Uplink	Any interface that connects switches to switches or switches to routers

FTE specific terms and definitions

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

Table 1-2 FTE Specific Terms

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	An FTE Community is 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, you can search *Knowledge Builder* glossaries – Server Glossary for Experion PKS systems and TPS_References for TotalPlant systems.

Additional references

Detailed installation instructions are not provided for all FTE components because these instructions are in the specific vendor's user manual. Because FTE can be installed on a variety of Honeywell node types, you may need to refer to your system implementation or installation guide for information that is not specific to FTE

The following table lists documents that may be helpful when installing or operating your FTE node.

Table 1-3 References for FTE Components

For more information on . . .	See this reference . . .
Cisco switches	For all user guides, go to http://www.cisco.com/ and search for "Cisco Catalyst"
Nortel switches	For all user guides, go to http://www.nortelnetworks.com/ and search for "BayStack 450"
Intel network cards	For all user guides, go to http://support.intel.com/support/network/adapter/ select the Adapter family and then Product Documentation
Allied Telesyn AT-MC102XL	**User Guide:** *AT-MC101XL; AT-MC102XL;AT-MC103XL; AT-MC103LH Fast Ethernet Media Converters Installation Guide* **Website:** http://www.alliedtelesyn.com/product/MC102XL
TPS installation	*TPS System Implementation Guide for Windows 2000*
Experion PKS installation	*Experion PKS Software Installation and Upgrade Guide*

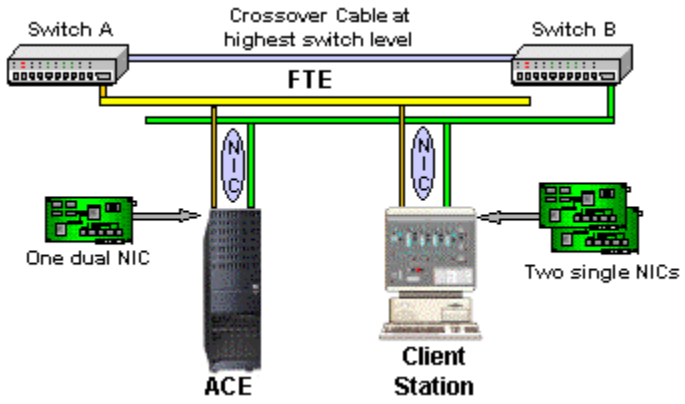
1.2 Fault Tolerant Ethernet (FTE) Functional Overview

Honeywell Fault Tolerant Ethernet (FTE) description

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

Fault Tolerant Ethernet (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.

Figure 1-1 FTE Dual Network Connections



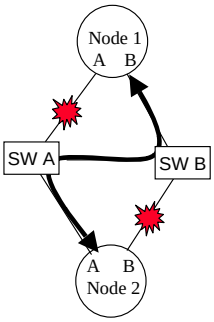
Communication between FTE nodes

The following figure 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.

Figure 1-2 FTE Node Communication

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 == channel is broken



Fault recovery information

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

Table 1-4 Fault Recovery Information

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 $N > 0$.

Using FTE with existing systems

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

FTE transmission support

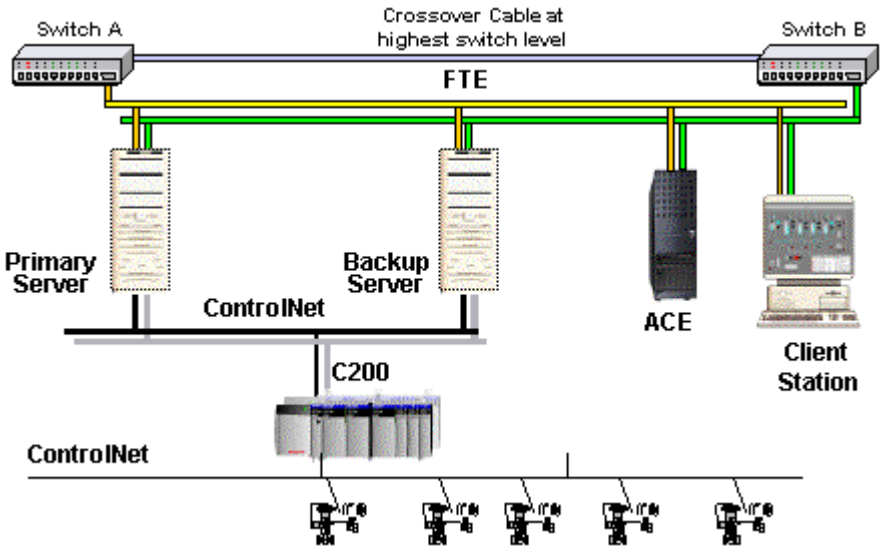
FTE supports the following two types of application traffic:

- Unicast (TCP/IP and UDP/IP), and
- 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 switches are inter-connected using one crossover cable. The FTE Network contains other redundant networking components such as switches, cabling, and redundant network interface adapters. Figure 1-3 shows an example of a basic FTE network.

Figure 1-3 FTE Network Topology



FTE Community

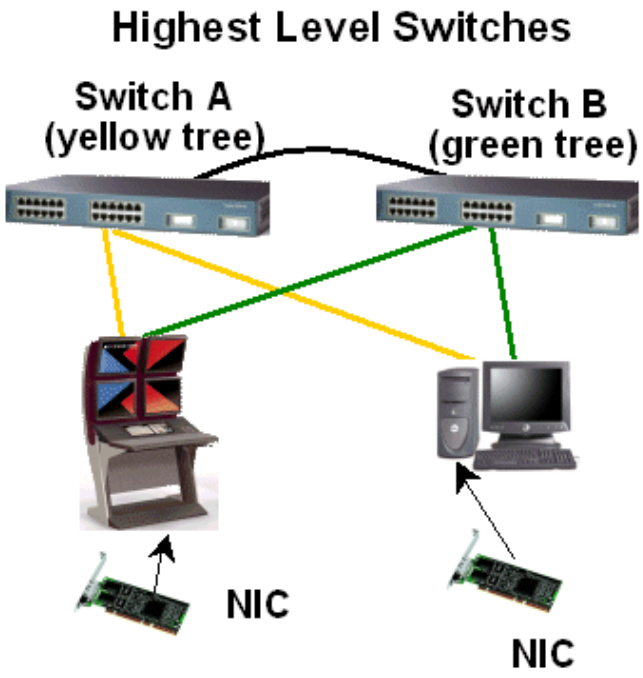
An FTE Community is a group of nodes within the same broadcast domain. Nodes that are single attached or dual attached with or without FTE may be members of the FTE community. FTE nodes are dual connected nodes that have fault tolerant communication coverage using FTE test messages. Non-FTE nodes are single or dual connected nodes that do not have FTE. Honeywell does not recommend multiple FTE communities within the same broadcast domain. Experion systems will not operate properly with multiple FTE communities in the same broadcast domain.

FTE Tree

FTE topology is two parallel tree hierarchies of switches, up to three levels, connected at the top by one crossover cable to form one fault tolerant network. The highest level switches are interconnected to a single FTE network. The separate physical identity of the two trees is maintained by color coding and tagging of cables, switches and FTE node ports.

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

Figure 1-4 FTE Trees



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 Experion PKS grouping is a collection of nodes associated with the same process unit. That is, a server, stations, and controllers, which typically have high intercommunication. Preferably, to minimize the number of switches and the amount of wiring between nodes in a grouping, all of a grouping's nodes would connect to the same pair of switches. If that is not possible due to plant topology, nodes in a grouping can be connected to different switch pairs and communications will still function properly.

FTE nodes

FTE nodes are those with the necessary redundant media components and Honeywell FTE software. FTE nodes connect to the LAN using redundant network interface adapters (each port has a unique IP address). FTE Nodes are resilient to single Ethernet failures such as switch or cable faults, and are able to communicate as long as at least one path exists between them.

FTE media components

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

2. Planning a Honeywell FTE Network

2.1 Before you begin

Assumptions

Users installing and configuring an FTE network should know networking concepts and requirements, including design, maintenance and security. This would include network administrators and control engineers.

Network services consulting and support for FTE

The Global Project Operations Networking Group has the upfront responsibility to deliver 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.

Tasks for planning an FTE network

Consider the following network requirements before installing your FTE network.

Table 2-1 FTE Network Planning Tasks

✓	Task
	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 Node's IP addresses.
	Verify software and media requirements.
	Plan IP address distribution

2.2 FTE Network infrastructure

An FTE network is comprised 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.

Plant Network levels

A plant network has four layers or levels. The following table briefly describes these levels. Level numbers are used to simplify the description of the node location within the network hierarchy. The FTE network of an Experion PKS system includes levels 1 and 2. Sections 3 through 0 of this document provide further details on these levels, including specific network best practices for each level.

Table 2-2 FTE Network Levels

Level	Description of Nodes in this Level	Go to
Level 1	Real Time Control (controllers and IO)	Section 3
Level 2	Supervisory Control, Operator HMI (HMI, and Supervisory Controllers)	Section 4
Level 3	Advanced Control and Advance Applications (Non Critical Control Applications)	Section 0
Level 4	Plant Level Applications (MES and MRP)	Section 0

FTE communities

An FTE community is a group of nodes that can 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 are single attached or are dual attached but do not run FTE may also be members of the FTE community. Experion systems will not operate properly with multiple FTE communities in the same broadcast domain and Honeywell recommends each FTE community be in a separate broadcast domain.

Maximum nodes within an FTE Community

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

Table 2-3 Single & Dual Connected Nodes in FTE Community

Single or Dual Connected	Characteristics	Network View
Dual connected node with FTE driver software	Node shares the same multicast address, UDP source port and UDP destination port as the other FTE nodes within the same community.	Seen as one FTE node when it shares the same multicast address. If the node is outside the multicast scope, it is seen as two non-FTE nodes.
Single connected Ethernet nodes	Node can be communicated with.	Seen as one non-FTE node

Large FTE systems

The maximum FTE node numbers do not prohibit large systems as FTE communities can be interconnected using a router. Individual FTE communities should be designed to include those nodes that have critical intercommunication requirements. Distributed Server Architecture (DSA) can be used to share data between routed FTE communities. Using this technique, a very 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 installation of 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

- Local peer-peer control is most important
- Peer to external peer is next most important
- Controller to server/station is next most important
- Server to station, ACE and other Level 2 nodes is next most important.
- Communication from Level 2 to Level 3 is generally less critical and more restriction can be placed on this path.

FTE critical configuration items

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

Table 2-4 FTE Critical Configuration Items

	Requirement	See
✓	Level 1 nodes must not have a default router 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.	
✓	Use DHCP or BootP for all non-Honeywell nodes.	
✓	Private IP addresses should be used where possible with NAT to corporate networks.	
✓	Level 1 addresses should be in a subnet separate from other Level 2 nodes.	

Table 2-4 FTE Critical Configuration Items

	Requirement	See
✓	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.	
✓	Router at Level 3 device that interfaces to level 2 devices MUST have no ip proxy-arp configured.	
✓	Switches are configured with the Honeywell configuration files.	Section 9
✓	Experion PKS nodes and switch/router uplinks (downlinks) must be connected to appropriately configured interface ports on the switches.	

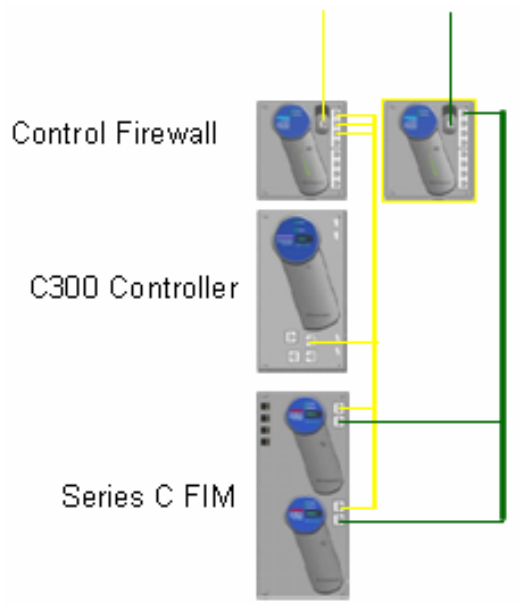
3. Level 1

3.1 Level 1 nodes

Level 1 nodes are the heart of the control system. This network segment contains controllers, FTEB-based I/O, and Series A or Series C FIM nodes.

Series C Level 1 LAN cluster

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



Citizenship:

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

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

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. 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. Attach the uplink of the Honeywell Control Firewall to a Level 1 or Level 2 Cisco switch using an interface configured as an uplink. You cannot cascade Control Firewalls – that is one Control Firewall cannot be connected to another.

ATTENTION

PC nodes, including temporary debug laptops, must not be attached to the inside of the Honeywell Control Firewall. The NETBios return messages will be blocked and the PC node will become the master browser. This will prevent proper file sharing to occur on the entire network.

NOTE: ICMP messages are blocked. This means that common debug applications like Ping and Traceroute will not work.

Honeywell Control Firewall features

The Honeywell Control Firewall has the following features:

- Allows only CDA connected traffic through by 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

C200 with FTEB best practice

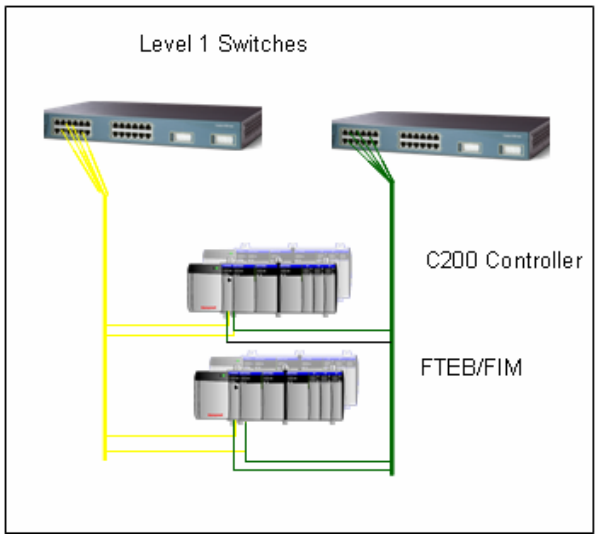
Installations with C200 controllers connected to FTE with the FTEB must be connected to a Cisco switch with a Level 1 configuration installed. Several settings in the Honeywell switch configuration files enable protection for Level 1 traffic. Other best practices include:

- TCP ports that are used for critical control and display traffic will be fixed and well known. Reception of a packet with those TCP port values informs the Cisco switches 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 cut off, but other traffic is not affected.

The use of a separate IP address range for Level 1 nodes is no longer recommended as a best practice due to the difficulty of configuration. This scheme is still recommended for those installations where Level 1 address reuse is required and is discussed in Section 8.3, “Reusing IP addresses for Level 1.”

Series A Level 1 LAN cluster

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



Citizenship:

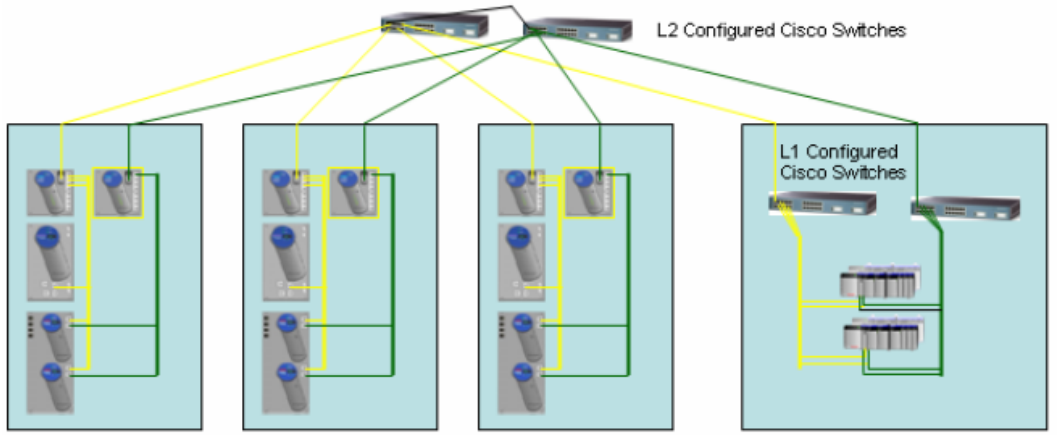
- Controller (C200)
- Fieldbus Interface Module
- Cisco switches

Level 1 Switches:

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

Connecting Level 1 LAN clusters

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



Citizenship:

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

Cisco Switches:

- Connect Level 1 clusters
- High reliability configuration:
  - 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
- Dual Cisco switch faults impact *inter-cabinet* traffic only

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 will have the shortest communication path. If this is not possible because of size or geographic dispersion, then their communications may 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:

- The 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 will 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, then the interface is cut off until the traffic level falls below 18%. Normal FTE traffic of broadcast and multicast is well below 2% for each.

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 effectively has 22 ports versus 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. See Section 9.6, "Honeywell's switch configuration files" for a description of switch configuration options.

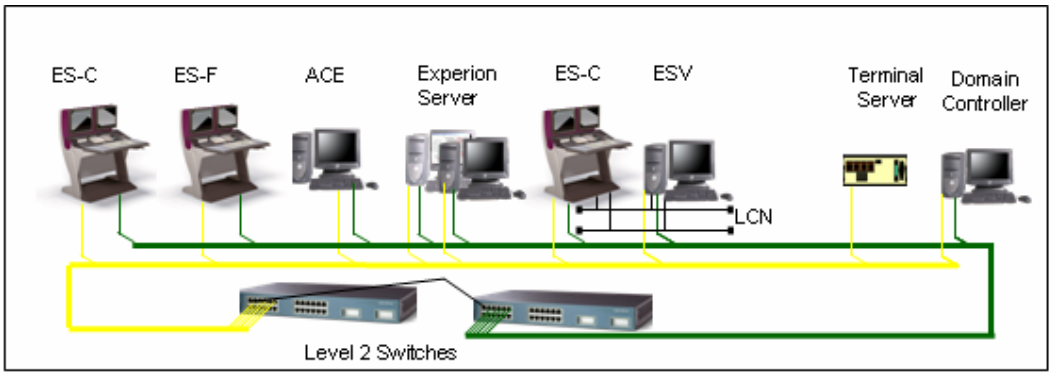
4. Level 2

4.1 Level 2 nodes

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

Level 2 LAN

The following diagram shows an example of Level 2 LAN.



Citizenship:

- Experion Server
- Experion Console
- Application node
- Subsystem Interfaces
- Domain controller
- Cisco switches

Level 2 Cisco switches:

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

4.2 Level 2 best practices

The nodes that reside on Level 2 are more susceptible to attacks by viruses or software glitches because of the open nature of the operating system and the customized software that is running on these nodes. For this reason, 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 35.

Level 2 switch configuration

The following are configured in the Cisco switches:

- Protection from broadcast and multicast storms on the interfaces to these open nodes.
- The display traffic, like the control traffic, is given a higher priority so the view to the process traffic takes precedence over other traffic on the switch. This is especially important if there is a “bad actor” on the LAN that is generating high traffic - the higher priority control and view traffic will arrive at first.

Avoiding multiple network connections

Avoid connecting a PC type node to multiple networks. For example, connecting a server to two networks turns the PC node into a router, which is a poor practice. Instead, the Experion network structure provides for the use of routers to join Level 2 nodes to Level 3 networks or to other Level 2 networks. 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 can be used for private connection to a single Ethernet device. An example is the Honeywell DHEB for bridging to the Data Hiway.

Non-FTE dual attached nodes within Level 2

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

- Terminal servers
- OPC servers
- PLCs

Non-FTE single attached nodes within Level 2

Non-FTE single attached nodes such as terminal servers or subsystem devices also can connect to Level 2 switches. For a large number of single attached nodes, a separate switch can be used to aggregate these nodes. Following are guidelines for using a switch for this purpose:

- The switch will count as a level for spanning tree purposes so it must not be connected to an FTE switch that is at the third level.
- The switch must not be connected to any Level 1 switches.
- The switch can be connected to either the *yellow* or *green* side, but the *yellow* side is preferred.

Nodes with embedded operating systems

Nodes with embedded operating systems may not have enough processing power to handle the volume of multicast and broadcast traffic generated by FTE test messages and Address Resolution Protocol (ARP) packets. This type of node must either be connected at Level 3 or protected with Access List filtering on a separate Level 2 switch. We recommend you use a qualified Experion switch for this purpose. Consult Honeywell Network Services for proper switch configuration.

Critical nodes

Honeywell recommends certain critical nodes, such as Safety Manager, be placed on a separate switch. Refer to “Safety controller best practices” in Section 4.3.

Best practices for connecting a crossover cable

FTE networks require a single crossover cable at the top of the hierarchy. In large systems we recommend that a 1 Gbps connection be used because in the case of multiple faults backbone traffic will pass through this connection. Consequently, the highest bandwidth must be available for this traffic.

To determine if you need capacity greater than 100 Mbps for the crossover cable, add the total average bandwidths of all the cluster servers. If the amount is greater than 20 Mbps, then we recommend you use 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 as long as the rule of 3 levels of switches is preserved. Do not connect the crossover cable to a Level 1 switch.

4.3 Implementing Level 2 best practices

Separate IP address ranges

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

- Servers on Level 2 need access to nodes on other subnets as well as access to certain nodes on Level 3 and possibly Level 3.5, or DMZ. Communication to other nodes may include Distributed Server Access (DSA), as well as engineering access to load control schemes and high-level control.
- Windows Server 2003 domain controllers are qualified to run the FTE driver. For a higher level of security, we recommend 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.
- Other nodes on Level 2 do not need to be accessed by other nodes on Level 3 and should be protected from such access.

Using filters in Level 3 routers

To control node access, filtering is used in 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 non-server nodes to communicate with Domain Controllers for authentication and name service.
- Allow Level 2 nodes to initiate communication with Level 3 Domain Controllers.

Domain controllers in an FTE network

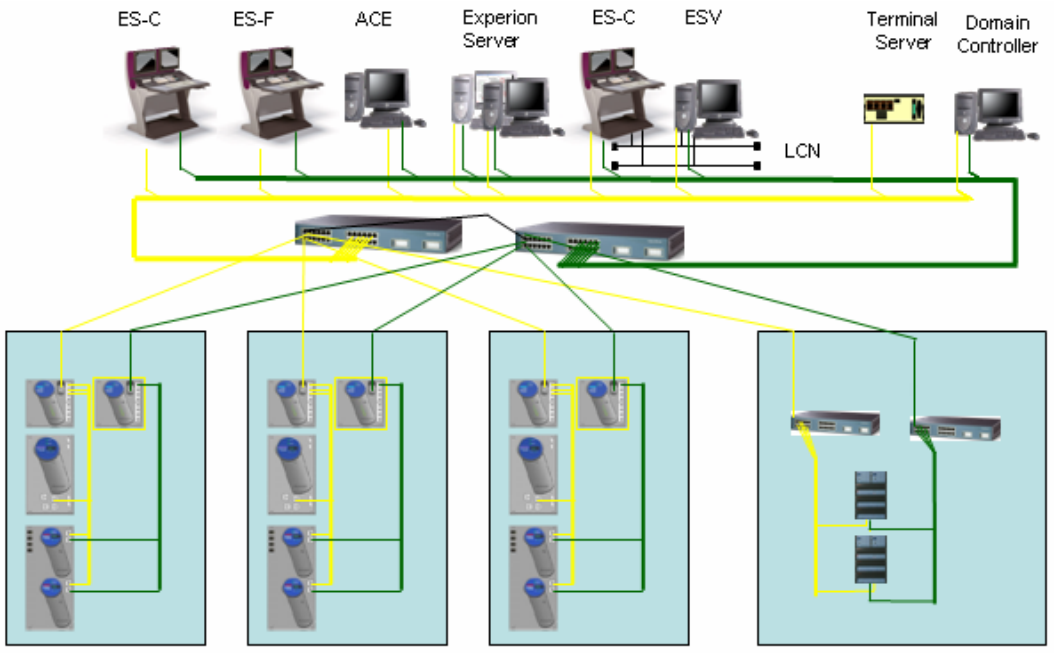
Windows Server 2003 domain controllers are qualified to run the FTE driver. For a higher level of security, we recommend a peer domain controller on Level 2. The Domain Controller must be addressed in the server range if complete communication with a root domain controller on Level 3 is needed.

For communities that don't need this extra level of protection, or when the local domain controller is offline, you can provide communication between Level 2 nodes and Level 3 Domain Controllers by adding access lists that enable *established* communications to return TCP packets from the Level 3 nodes to the initiating Level 2 nodes.

In either case, the established communications is needed 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 that can be used for filtering.

Connecting Level 2 to Level 1

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



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

Level 1 Cisco switches:

- Prioritize ingress traffic; non-CDA in low priority queue
  - Ensures Level 2 to Level 1 supervisory traffic cannot disrupt Level 1 control

Level 2 Cisco switches:

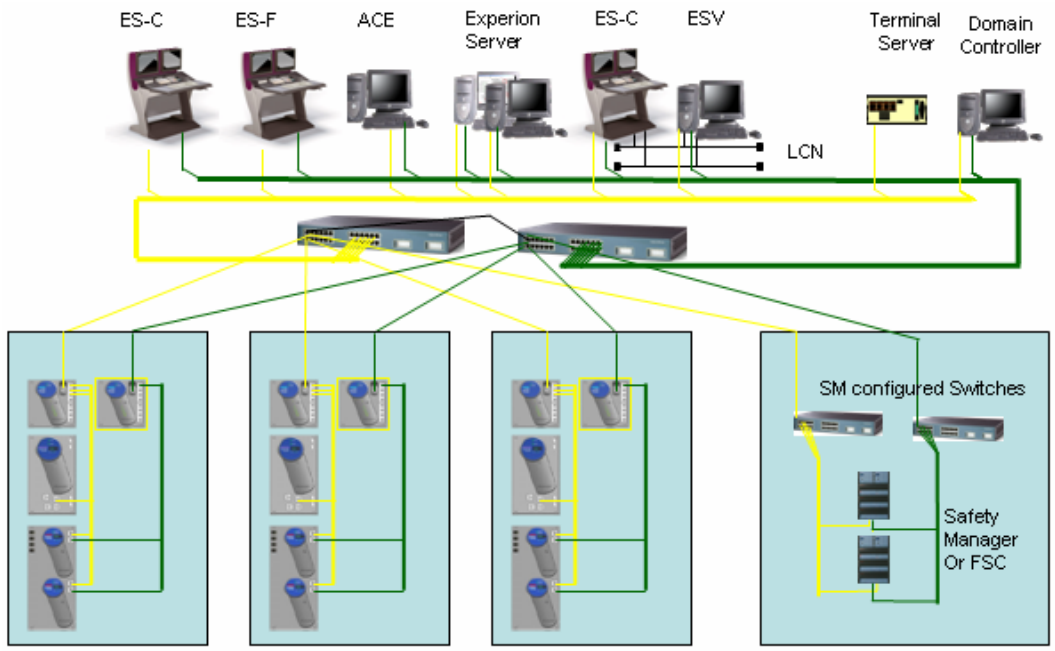
- Provide Level 1 to Level 2 connectivity
- Broadcast, multicast storm suppression
- Preconfigure CDA traffic in high priority switch queue (that is, ACE-ACE, ACE-Cx, ACE-FIM, Server-Cx, Server-FIM)
- Preconfigure non CDA traffic in low priority switch queue

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 how they are used in a system. The following sections contains recommendations based on the safety controller's role in the system.

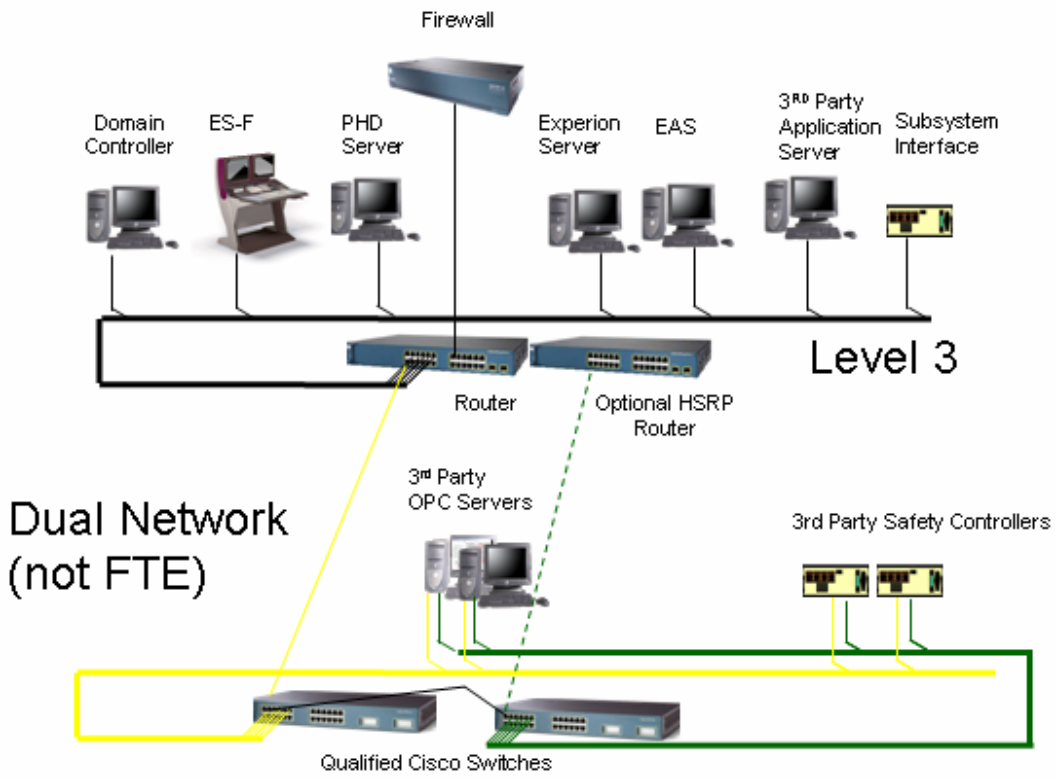
Systems with peer-to-peer control communication

For systems in which there is peer-to-peer control communication with the process-connected controllers such as the C300, the safety controller must be connected to the same FTE community as the C300/C200 controllers. These are critical nodes and we recommend they be protected in the same manner as Level 1 nodes by using a separate switch. The switch configuration should be the same as that for Level 1 switches being used for systems with FTE-based controllers or I/O. Systems with C300s will need configurations specific to the controller. Honeywell Network Services can provide support for these configurations.



Systems using SCADA data only

For systems in which SCADA data only is used, we recommend the safety controller be placed in a separate subnet that is 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.



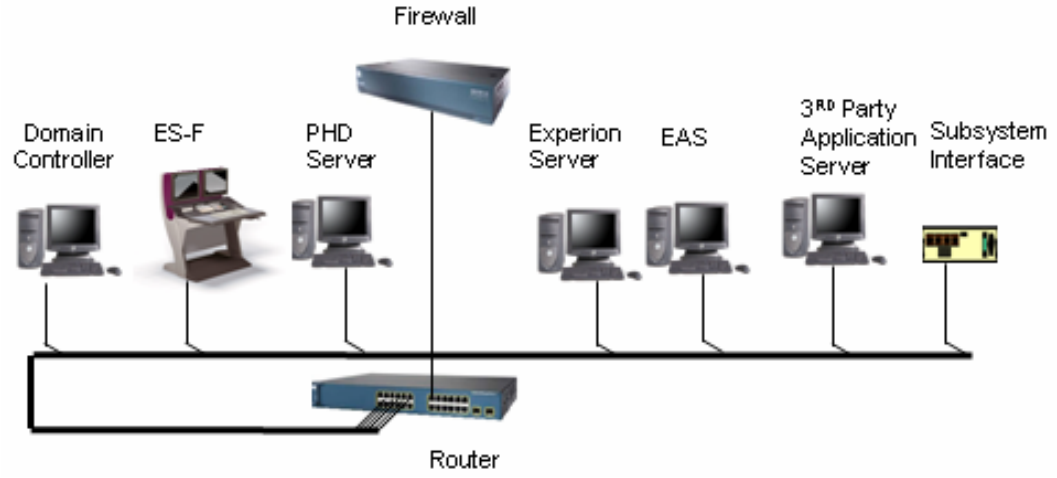
5. Level 3

5.1 Level 3 nodes

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

Level 3 LAN

The following diagram shows 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

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

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 through use of 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.
- The use of unicast for DSA keepalive messages is the recommended best practice.
- If you must use multicast, which is less 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 may also use multicast addresses as described in the “Using Redirection Manager (RDM) with Level 3” on page 47.
- 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 47.
- Configure access list filters for the FTE communities that:
  - Permit complete access only to the server IP range, and
  - Allow *established* access to the remainder of the FTE subnet.
  - Deny all other access to the FTE subnet.
- If not using SFP/GBIC connections, configure the FTE switch’s router interfaces for 100-megabit full duplex.
  - **NOTE:** The router must be connected to either a switch interface that is 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.

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 you 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, then a mechanism using ICMP must be selected. In this case, ICMP must be allowed between Level 3 nodes and subnets.

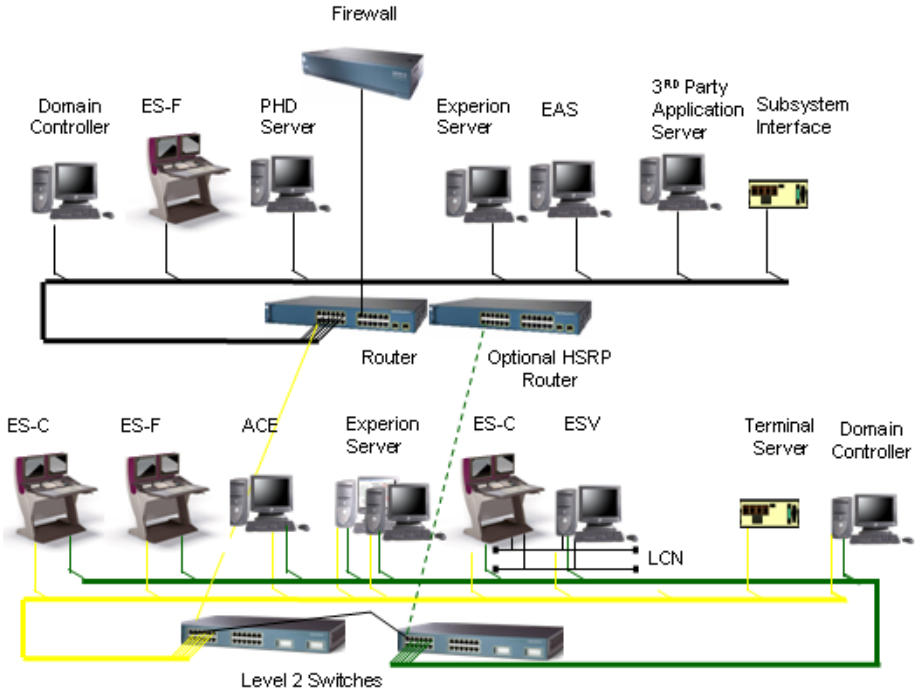
5.3 Level 2 to Level 3 best practices

Best practice for multiple connections from Level 2 to Level 3

If you require dual connections between the FTE backbone switches and Level 3, the best practice is to use two routers that are 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. We recommend you consult with Honeywell Network Services for correct router configuration.

Connecting Level 2 to Level 3

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

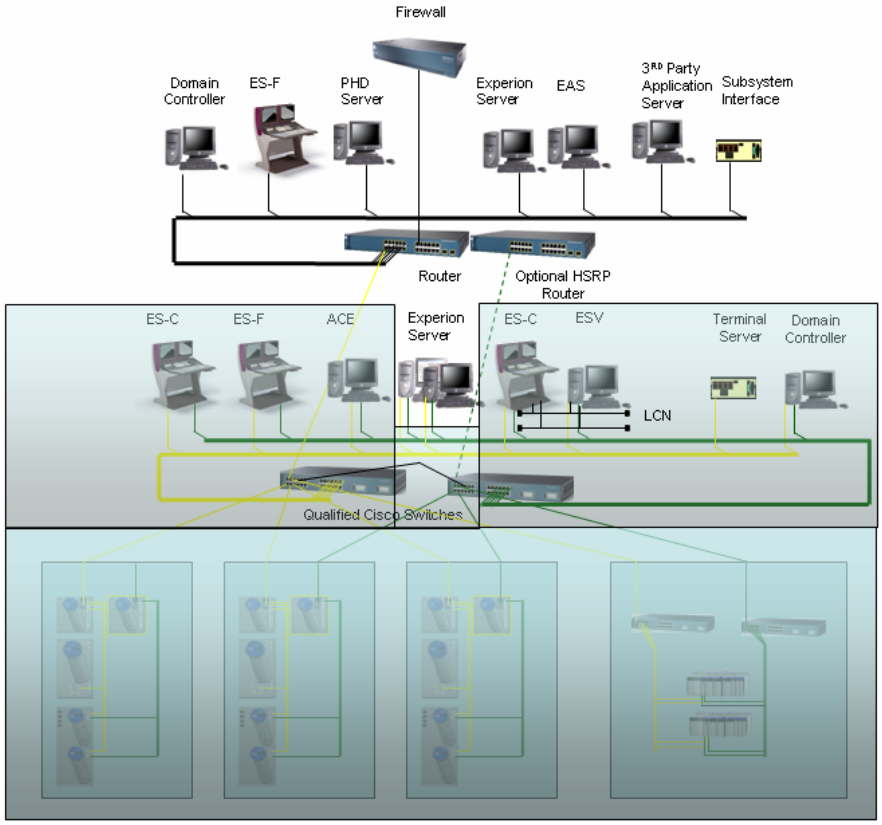


Routers and filter:

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

View of Level 2 from Level 3 with router and filter

The following diagram shows Level 3's view of the Level 2 LAN when a router and filter are used. Nodes not visible are shaded in gray. Notice that only the Experion Servers are visible to Level 3 as these are the only nodes that have been allowed in the filter. None of the Level 1 nodes are visible to any 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 DCs and L2 nodes requiring authentication)

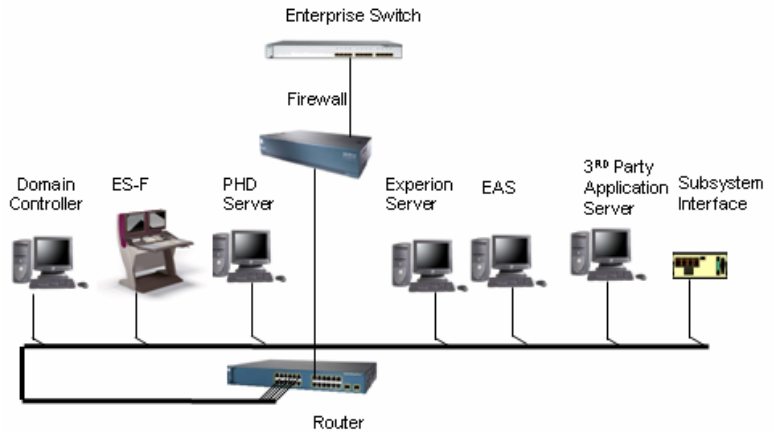
6. Level 4

6.1 Level 4 nodes

Level 4 is not 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.

Process Control Network to business network

The following diagram shows the connection of the PCN to the Level 4 (business network) through a firewall and router.



6.2 Level 4 best practices

Because Level 4 is a different security and networking environment, Honeywell strongly recommends that Level 3 and Level 4 be separated by a firewall. Not allowing data to cross more than one network level is a general best practice, and it is especially important for Level 3/Level 2 to be protected from Level 4. For this reason Honeywell recommends you a demilitarized zone (DMZ). See “Establishing a DMZ” on page 53.

6.3 Implementing Level 4 best practices

Firewall requirements

Requirements for a firewall between Level 4 and Level 1, 2 and 3:

- If there is a need to use DSA or any other form of communication with Level 2 that requires Microsoft RPC or DCOM APIs, then 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 or Level 2, but again, direct communications between Level4 and Level 3/Level 2 is not recommended.
- Level 1 nodes must not be allowed to communicate with nodes on Level 3 or on Level 4.
- Level 1 nodes may only communicate with Level 2 nodes on the same subnet.

Router configuration

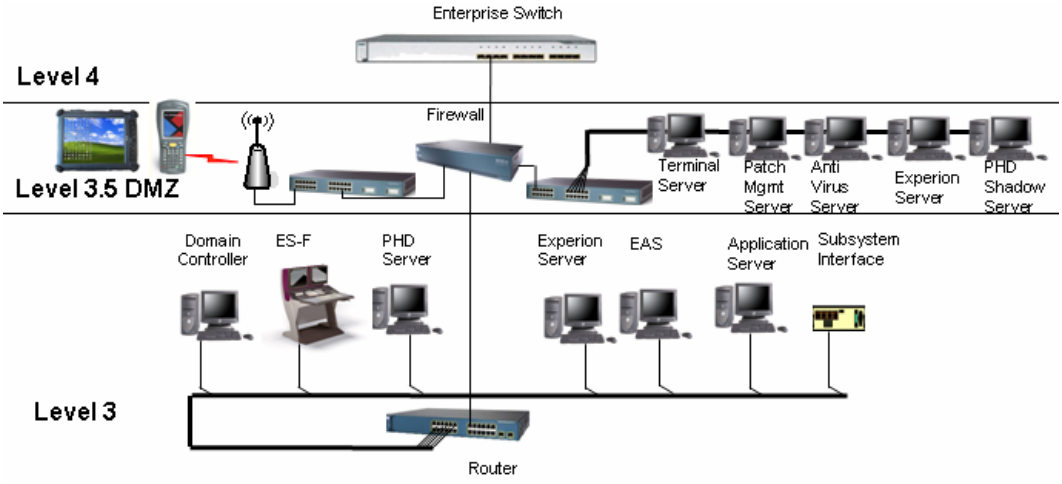
The router-to-firewall connection should be a single point of connectivity enabling higher security and improved management. A major advantage of this is the ability to pull a single cable to create an “air gap” between Level 3 and Level 4. The connection to the firewall isolates Enterprise LAN Broadcast and Multicast traffic while enabling connectivity between the PCN and Enterprise LAN.

Firewall configuration

The firewall enables a restrictive security policy for traffic between Level 4 and Level 3, and should deny all access to the PCN unless it is explicitly permitted. A best practice is to use IP address source and destination filtering. Only specific nodes on the enterprise network are permitted to communicate with specific nodes on the PCN. Permitted traffic must be limited to server-to- server traffic only (for example, Experion Server or PHD). TCP port filtering is recommended to stop denial-of-service attacks to well-known ports.

Establishing a DMZ

If Level 4 nodes need to access data on Level 3, Honeywell recommends you establish a DMZ or a Level 3.5 on which only those nodes on Level 3.5 can access those on Level 4. If necessary nodes from Level 3 and Level 2 can access those 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. Terminal servers and virus update file servers can also 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 and Level 4 and Level 3.5 and Level 3. For further information on establishing a DMZ, see the "Network Security" section in the *Honeywell Network and Security Planning Guide*.



Recommended communication restrictions

The following table lists 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

Legend	
NRC	Not restricted communication
LC	Limited communication
VLC	Very limited communication
NC	No communication

7. Additional Best Practices

7.1 Robust FTEB-based topology

Configuration rules for a robust topology

For critical peer-peer communications that cannot tolerate a communication delay of longer than 250 milliseconds following an FTE cable fault, the C200s and/or FTE connected FIMs should reside on the same switch pair. Beginning with R200, Experion PKS supported three different 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 three configurations together with the guidelines in this section should be followed when configuring FTE topologies for critical and non-critical processes using FTEBs and hierarchical switch configurations.

FTEB switch connection guidelines for critical process

For critical processes, the FTEBs should be connected to one or more switches separate from the switches used for Level 2 nodes. Considerations for peer-peer recovery times should be taken into account. These switches should be configured with the Level 1 configuration script.

For critical processes, the Level 2 Nodes should be configured on switches separate from those switches used for FTEB Modules. These switches should be configured with the Level 2 configuration script.

FTEB switch connection guidelines for non-critical process

For non-critical processes, the Level 2 nodes and Level 1 nodes may be connected to the same switch pair as described in Section 4. In this configuration Level 2 “mixed node” configuration script should be used. This configuration is typical for small cost-sensitive systems.

7.2 Variations on best practice

Remote locations

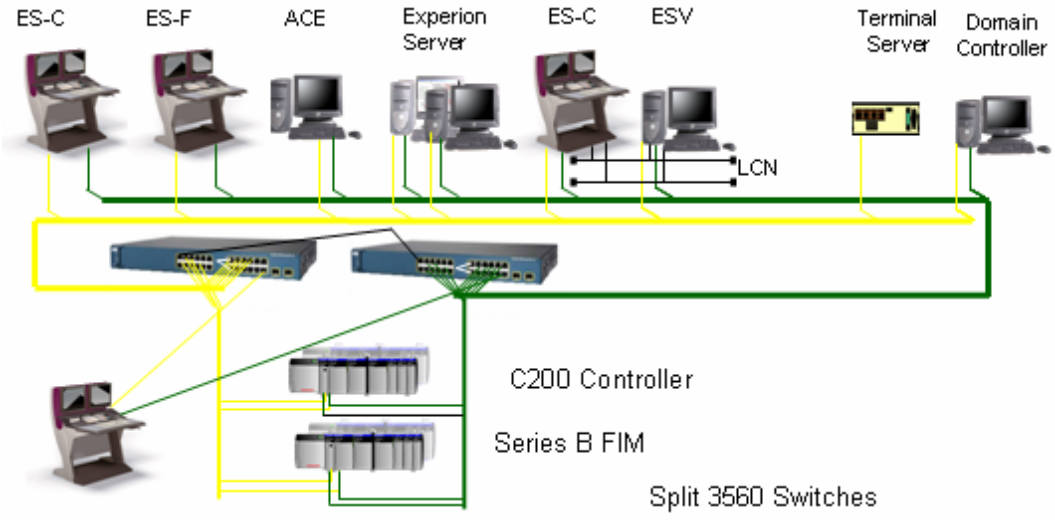
Due to geographic limitations you may need to modify Honeywell's best practice architecture. For example, you may need to add a Level 2 console station node at a satellite control area to allow a roving operator to view the process, or to allow view of the process in case of a catastrophic break in the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

System with station on split switches

In some instances, such as those previously described, it is acceptable to put 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:

- From Level 1 switches to local Level 2 switches, then
- 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 the Cisco 3560. This switch configuration, which is more secure than the previous "mixed" switch configuration, should be used.

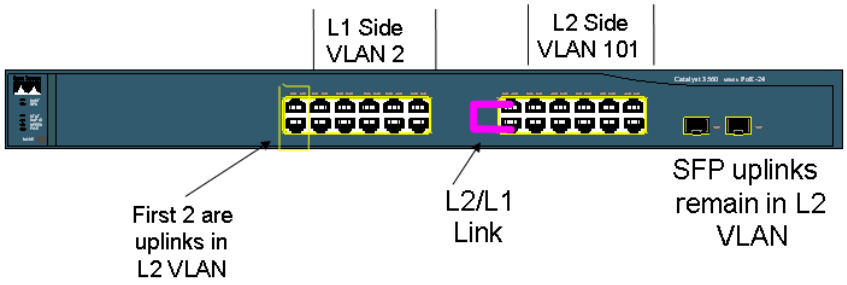


Split switch configuration

In a split switch configuration the switch is split in two sections: one for Level 2 and one for Level 1. Figure 7-1 shows 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
- 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.

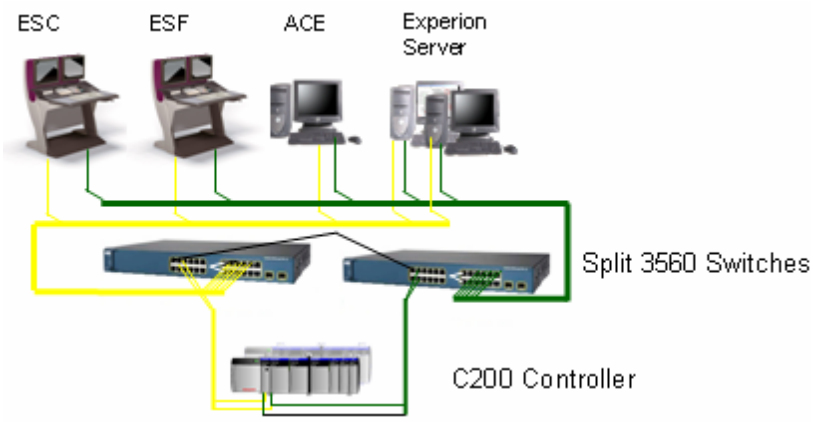
Figure 7-1 FTE Dual Network Connections



Small Experion systems with FTE

The Experion system is expandable from very small systems with only a few nodes to very 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 mixed switch configuration file would be used for this installation. Once the installation requires multiple layers of switches or is geographically spread, then the Honeywell best practice should be followed.

Figure 7-2 Small system with a single layer of switches

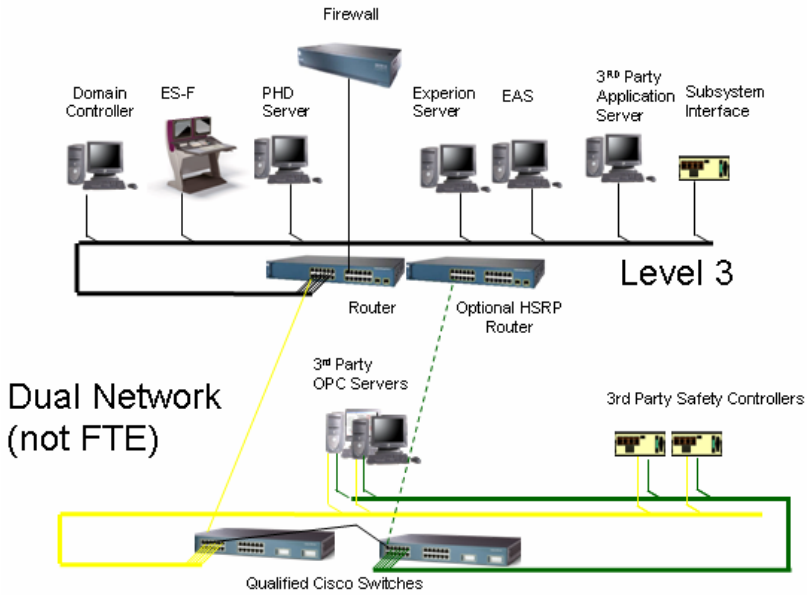


Third-party safety equipment

Third-party safety equipment may need to be directly connected 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 will need 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.

Figure 7-3 Peer-connected safety controller with OPC servers

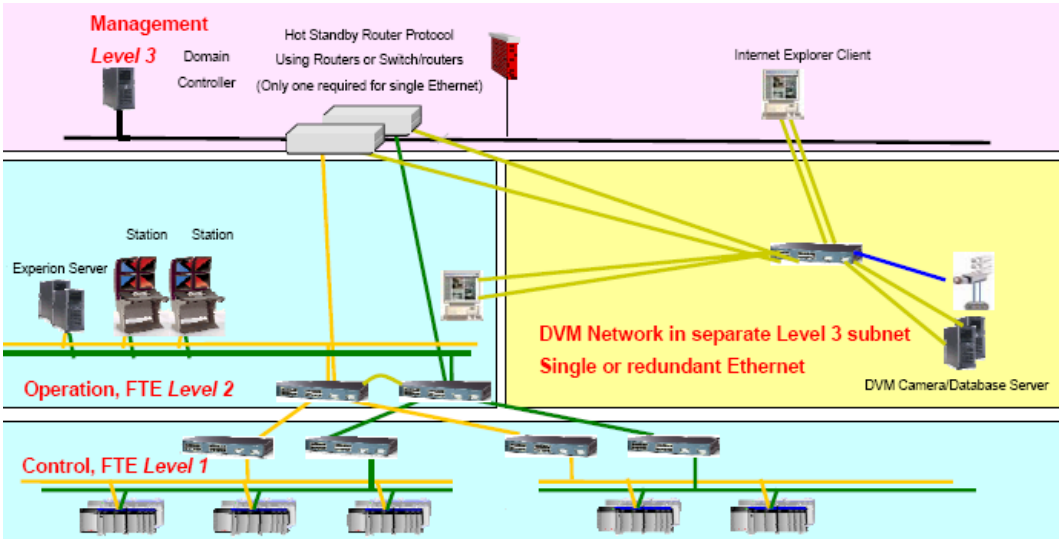


7.3 Digital Video Manager best practices

The Digital Video Manager (DVM) is capable of consuming a great deal of bandwidth, depending on the configuration. For this reason, Honeywell recommends the following best practices for DVM

- Create a separate L3 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 will trip storm limits in the Cisco switches

DVM network



7.4 TPS upgrade best practices

Existing TPS systems can be upgraded with Experion capabilities.

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 stand alone network, that is, 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 part of a plant wide network. In this case, the FTE network must be connected to the L3 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, meaning there is no router, or the existing router does not have the required filtering capability, then the FTE network must connect to L3 through a firewall with the same required filtering.
- A conversion of the PCN to FTE. In this case, the qualified FTE switches must replace existing PCN switches, and FTE software and dual NIC interface hardware must be added to the TPS nodes.

8. Use of IP Addresses in an FTE Network

8.1 Introduction

With the presence of controller nodes in the FTE community, you must pay careful attention to network communication reliability and security. Maximum security can be achieved by providing complete isolation in the form of an "air gap" between the control LAN and other plant users. This, however, is not feasible, as most installations require some level of communication between the control LAN and the plant LAN. Proper IP address management can provide the extra needed security when the control LAN cannot be completely disconnected from the plant LAN.

IP address ranges for FTE communities

Honeywell has developed several recommendations for IP address range selection to increase the security when connecting the Control LAN to outside communications 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
- 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

IP address range selection recommendations

The following table summarizes Honeywell's recommendations for IP address range selections. See subsequent sections for details on IP addressing requirements and examples for different LAN configurations.

LAN Description	Recommendation
Isolated FTE community	Follow the best practices of connected communities so if a router is needed at a later time, the IP addresses will already conform to Honeywell's best practices.
Multiple FTE communities isolated from Level 4 networks	Private IP addresses Simple address range configuration
FTE Communities connected to Level 4 with no COM communications	Private IP addresses with a firewall that performs Network Address Translation (NAT) for communication outside the plant control network. Dedicated equipment for the firewall. Placement of servers in a separate range from other Level 2 nodes.
FTE communities connected to Level 4 with COM communications	Unique Level 2 and Level 3 addresses that are compatible with Level 4 addresses. Do not use NAT. A method that conserves addresses, although it is more difficult to configure. A subnet size that covers all Level 2 nodes. A server range contained in the lower addresses that allows the other Level 2 nodes to start on a power of 2 boundary. A reserved subnet size that can be used for the largest Level 1 range in the plant.

IP addresses for non-Honeywell nodes

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

8.2 Recommendations for FTE Network communities

Isolated FTE community

Even if there is complete isolation of the control LAN from the IT LAN, IP address ranges and rules should follow the best practices of the multiple isolated or communities connected to Level 4. If the network expands so that a router is later needed, the IP addresses will already conform to Honeywell's best practices for connected networks.

Multiple FTE communities isolated from Level 4 networks

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

Octet	Description	Example
CN	FTE community number Multiple FTE communities can be connected with a router.	First FTE subnet would be 10.**1**.X.Y Second FTE subnet would be 10.**2**.X.Y

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.

Private address distribution ranges

An address range of **10.CN.X.Y** can be 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	First FTE subnet would be 10.**1**.X.Y Second FTE subnet would be 10.**2**.X.Y
X	Range of addresses where the two types of nodes exist. Servers must be in a separate range from other Level 2 nodes.	10.1.**0**.Y for server nodes 10.1.**1**.Y for station nodes 10.1.**2**.Y for any other nodes such as ACE, PHD and third-party IP based nodes.
Y	Any address between 1 and 255	10.1.2.**24**
Using the previous examples:		
If the FTE community is connected to a router, the router interface IP address should 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 should be in the address space above the other nodes on Level 2 and outside of the range of the subnet mask of the router interface, but within the subnet mask of the nodes that need to communicate.		Level 1 addresses would appear in the 10.1.4.Y range. Level 3 nodes must not be able to communicate with Level 1 nodes. The nodes will have the following subnet masks: • Level 2 Servers and console stations with communication to Level 1 nodes: 255.255.248.0. • Level 2 nodes with no communication to Level 1 nodes: 255.255.252.0. • Level 1 controller nodes: 255.255.248.0. • Level 3 router interface to Level 2: 255.255.252.0.

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. Even though it may be more difficult to configure, Honeywell recommends a method that conserves addresses, such as the following:

- Obtain a subnet size that will cover all of 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 boundary.
  - 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

Table 8-1 provides examples of the IP address distribution of an FTE community subnet containing:

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

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

Table 8-1 IP Address Distribution Example

IP Address	Description
164.1.0.1	The router VLAN IP address with subnet mask of 255.255.255.192: enough for 62 usable nodes, the subnet mask and the subnet broadcast address
164.1.0.2-15	Server nodes (5 servers 2 addresses each starting at address 2 rounded up to power of 2). The subnet mask is 255.255.255.128 to cover both Level 2 and Level 1 nodes
164.1.0.16-63	Stations, ACE terminal servers plus some spare addresses. The subnet mask is 255.255.255.128 to cover the Level 2 and Level 1 nodes.
164.1.0.64-127	FTEB (controller addresses must be outside of the subnet mask of the router interface). The subnet mask is 255.255.255.128 to cover the Level 1 and Level 2 range. The router interface to the FTE community blocks all access from Level 3 by the subnet mask of 255.255.255.192.

8.3 Reusing IP addresses for Level 1

Purpose

Level 1 devices may potentially consume thousands of IP addresses in a corporate IP address space. If you must conserve corporate IP addresses, we have provided a scheme for reusing IP addresses. This scheme, however, should only be used if IP address reuse is absolutely necessary and private IP addresses are not available. Do not use this scheme for standard network addressing.

Address reuse scheme for Level 1

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

- One range of addresses for Level 1-only should 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.
  - **NOTE:** Existing Level 1 nodes do not need to have their addresses changed.
- With the addition of static routes in R210SP2 and R300, private addresses such as 10.x.x.x or 192.168.x.x could be used for this reused address range.

Route add command

In order for Level 2 nodes to communicate with Level 1 nodes in the reusable address space, certain configurations must be implemented, including the use of the *route add* command and proper use of address ranges.

Route add command service

Experion R300 includes a new service loaded 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, then the static route to the controller will be added to the *yellow* interface. Every ten minutes, the service tests for changes in the server database, and to verify the static route is still connected to the *yellow* interface. Any errors or problems are sent to the application event log.

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:

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

Static route add command

For pre-R300 Level 2 nodes 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.

Route add example

The following example shows the command for a Level 2 node in which the:

- Level 2 address range is 164.1.0.0 to 164.1.7.255, and
- 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 address of the node being configured with the route add.

–p makes it persistent across reboots.

Results of route add command

The Level 1 nodes will receive the address range of the Level 1 nodes and the Level 2 nodes. The Level 1 nodes will 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, then
- The Level 1 range in the Route Add example would start 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 will be open to the Level 2 addresses.
- The range can be larger than the actual Level 2 address range because communications will not go outside of the FTE community subnet.

9. Installing and Replacing Switches

9.1 Introduction

The specific tasks you need to perform depend on the switch model number you are installing.

Prerequisites

Before performing the procedures in this section, it is assumed that you:

✓	Task
	Are aware 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
	Are aware of FTE media requirements
	Reviewed the *Fault Tolerant Ethernet (FTE) 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. **Note**: If the version is not the same as that listed in the SCN, contact Honeywell Network Services for the procedure to upgrade the IOS.

Qualified network equipment for use in an FTE network

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

9.2 Installing and configuring Cisco switches

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 *Yellow* Tree and one for the *Green* Tree) are required at the highest switch level and they MUST be interconnected.
Tree level	Two switches (one for the *Yellow* Tree and one for the *Green* Tree) are required to maintain redundancy.
Small FTE Network	Would typically have only one level of switches
Large FTE Network	May have an 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 switch can be expanded in increments of 12 ports, up to a maximum of 96 ports.

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 cut off - when it drops below 18 percent, communications is restored.

Ports that are connected to FTEB nodes do not have bandwidth limits, as the link speed is already lower than the 20 Megabit level. Uplink (or downlink) ports come from a switch source so storm suppression is not needed.

Expanding an existing FTE network

Nortel switches may continue to be used if already installed. However, controller nodes must be connected to qualified Cisco switches, and may not 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 that is 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, the Cisco switches must be at the top of the switch hierarchy and the Nortel switches must connect into the Cisco switches.

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 can occur if a loop is created in the switches, and with controllers in the system, this increased protection is critical. Spanning tree should remain disabled for existing Nortel switches in an FTE community.

CAUTION

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

Cisco switch 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	"Port fast" spanning tree enabled	Allows quick reconnection
Level 2 100 Megabit nodes	"Port fast" spanning tree enabled	Allows quick reconnection
Uplink/downlink ports	Normal spanning tree enabled Must have the speed set to 100 Megabit and full duplex	Cisco does not recommend using this feature when connecting to other switches. The exception is the GBIC based ports, which do not have the problem of locking on the wrong speed or duplex.
Ports connected to Microsoft based nodes	Must have the speed set to 100 Megabit and full duplex	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 auto and the duplex set to full.	

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 of this guide.

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 connection.

Switch power source

CAUTION

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

9.3 Replacing switches

Switch migration requirements

The following table lists qualified Experion switches and indicates the switch migration requirements.

Table 9-1 Switch migration requirements

Honeywell Switch	1st released in Experion	Migration needed for R300?	Migration needed for R301?
Cisco 2950G-24	R201	No	No
Cisco 2950G-48	R201	No	No
Cisco 3550-12G	R201	No	No
Cisco 2955C-12	R210	No	No
Cisco 3550-24-FX	R210	No	No
Cisco 3560-24-TS	R300	N/A	No
Cisco 3750G-12S	R300	N/A	Yes for stacked
Cisco 2960-24TC	R301	N/A	N/A
Cisco 2960-48TC	R301	N/A	N/A

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.
- Configure switches offline using the switch configuration files provided by Honeywell before beginning the replacement procedures.
- If you are replacing both switches, replace the B switch first; replace the A switch second.
- Always verify the switch replaced first is operating correctly before replacing the second switch.
- If you are replacing a switch in a stacked configuration, follow the guidelines in Section 9.4, “Stacking Switches.”

Special considerations when replacing stacked switches

3750-12s switches that are stacked have a vulnerability when 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 back 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 the .bin file will result in the switch not spreading the new IOS to the other switches in the stack.

Tasks for configuring and replacing switches

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

✓	Task
Configure new switch A-yellow (offline)	
	See “Connecting locally to the switch” on page 103.
	Verify the switches have the IOS version qualified by Honeywell as listed in the SCN for your release. **Note**: If the version is not the same as that listed in the SCN, contact Honeywell Network Services for the procedure to upgrade the IOS.
	See “Configuring switch interface options” on page 104.
	See “Loading the switch configuration file” on page 111.
Configure new switch B-green (offline)	
	See “Connecting locally to the switch” on page 103.
	Verify the switches have the IOS version qualified by Honeywell as listed in the SCN for your release. **Note**: If the version is not the same as that listed in the SCN, contact Honeywell Network Services for the procedure to upgrade the IOS.
	See “Configuring switch interface options” on page 104.
	See “Loading the switch configuration file” on page 111.
Install new switch B-green	
	If necessary, label network cables with the switch port type they are connected to.
	Shut down existing *switch B green.*
	If switch pair is **not** at the top level, remove the uplink cable from existing *switch B green.*
	If switch pair is at the top level, remove the crossover cable from existing *switch B green.*
	Disconnect network cables from *switch B green*.
	If switch pair is **not** at the top level, connect the uplink cable to the new *switch B*

✓	Task
	green.
	Connect network cables to the new *switch B green* verifying you are connected to the correct switch port type.
	If switch pair is at the top level, connect crossover cable to the new *switch B green*.
	Turn on *switch B green* and verify the new *switch B green* is communicating.
Install new switch A-yellow	
	Shut down existing *switch A yellow.*
	If switch pair is **not** at the top level, remove the uplink cable from existing *switch A yellow.*
	If switch pair is at the top level, remove the crossover cable from existing *switch A yellow*.
	If necessary, label network cables with the switch port type they are connected to.
	Disconnect network cables from existing *switch A yellow.*
	If switch pair is **not** at the top level, connect the uplink cable to the new *switch A yellow*.
	Connect network cables to new *switch A yellow* verifying you are connected to the correct switch port type.
	If switch pair is at the top level, connect crossover cable to the new *switch A yellow*.
	Turn on *switch A yellow* and verify the new *switch A yellow* is communicating.

9.4 Stacking Switches

About stacked switches

A stackable switch configuration allows two or more switches to be clustered in such 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.

Figure 9-1 FTE stacked switches for yellow and green tree

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 then adding the stacked switch to the network. Following are the tasks associated with stacking switches in an FTE network.

No	Task
1	Power up and connect to the first base switch. See “Connecting locally to the switch” on page 103.
2	Verify the switches have the IOS version qualified by Honeywell as listed in the SCN for your release. **Note**: 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 no switch added to the stack must have an IOS that is newer than the qualified version.
3	Configure the base switch. See “Configuring switch interface options” on page 104.
4	Load the switch configuration file on the base switch. See “Loading the switch configuration file” on page 111.
5	Power up the next switch to be added to the stack (do not connect it at this time) and verify it has the correct IOS version. See “Checking the switch IOS” on page 85.
6	Power down the switch and then connect it to the stack. See the 3750-12s User Manual for connection procedures.
	**CAUTION** Always verify the switch is powered off before connecting it to the stack. Connecting a switch that is powered on may cause other switches to reload and change their configuration.
7	Add the switch to the stack by typing the `Conf t` and `Switch X provision ws-3750-12` commands at the switch prompt, substituting the switch number in the stack for X. For example: `C3750-G1#`**`Conf t`** `C3750-G1#`**`Switch 3 provision ws-3750g-12`**

No	Task
	TIP 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 85.
9	Load the new switch configuration file to the stacked switch. See “Loading the switch configuration file” on page 111.
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#  Role      Mac Address     Priority     State`
	`-----------------------------------------------------`
	`*1       Master    0015.faa3.8800     3          Ready`
	`2        Member    0015.faa3.bf00     2          Ready`
	`3        Member    0017.94b2.6800     1          Ready`
	All switches in the stack should indicate a status of **Ready**.

12	Configure the switch priority to increase the chances the base switch will remain the master switch. See “Configuring switch priority in a stacked switch” on page 87.

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 newest version available, which may not be the version qualified by Honeywell. Switches with an unqualified IOS may have unpredictable performance. Use this procedure to check the IOS version.

Step	Action
1	Telnet to switch.
2	Enable and log in to the switch.

3	Check the IOS version by typing `show boot` at the switch prompt.
	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	If the IOS version is not the one qualified by Honeywell as listed in the SCN for your release consult with Honeywell Network Services for the procedure to upgrade the IOS.

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 the .bin file will result in the switch not spreading the new IOS to the other switches in the stack.

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.

Step	Action
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.

Step	Action

3	Identify the switch order in the interface range command:
	`interface range GigabitEthernet2/0/1 – 12`
	For example:
	Change the 2 following GigabitEthernet to a 3 to identify the third switch in the stack.
	`interface range GigabitEthernet3/0/1 – 12`
	Note: 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 Hyperterm'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 the .bin file will result in the switch not spreading the new IOS to the other switches in the stack.

Configuring switch priority in a stacked switch

Configuring the switch priority increases the chances the base switch will remain the master switch. Use this procedure to establish specific priority for each switch in the stack.

Step	Action
1	Serial connect or telnet to the switch.
2	Enable and log in to the switch.
3	Type `Conf t` at the switch prompt.
3	Type `Switch X priority XX` at the switch prompt, substituting the switch number for X and the priority order for XX. Note: 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 9-5 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, see the *Honeywell Control Firewall User's Guide*.

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. Because Honeywell Control Firewalls do not use spanning tree, interfaces connected to Control Firewalls will be 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.

Honeywell Control Firewall guidelines

- Connect Honeywell Control Firewalls to switch interfaces configured for Level 2 host nodes - in other words interfaces where you would connect a computer, and configure the interface as follows:
  - Type: portfast
  - Type speed: 100
  - Type duplex: full
- If you do connect a Honeywell Control Firewall to a top level switch such as a 3750 or 3650 configured for all uplink ports, verify the Control Firewall interface is configured for portfast.
- Verify no other connections of Cisco to Cisco switches are configured for portfast – only those used for Honeywell Control Firewalls.

Honeywell Control Firewall connection requirements

- 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.

Benefits of Honeywell Control Firewalls

A Honeywell Control Firewall provides the following benefits:

- Blocks messages that Level 1 nodes should 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 R300 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 very simple switch with eight device ports and one uplink port. Its functions are so simple it does 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 a set of switch configuration files available on the Experion PKS Application Software DVD and the Common Component CD for TPS users. When implemented, these files configure the FTE switch ports for different node types according to defined requirements. See Table 9-5 for a complete list of all these files.

Switch configuration requirements

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

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 enabled
FTE Node	Enable	Full	100 Megabit	Port fast spanning tree enabled
GBIC based ports	Enable	_____	1000 Megabit	Normal spanning tree enabled
CF9	Enable	Full	100 Megabit	Port fast spanning tree enabled

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 three types of switch configuration files:

Table 9-2 Network requirements for each level

Network Level	Requirements
Level 1 only	To help protect against network problems, the Level 1-only switches have the following tighter limits on incoming traffic: • Uplink inbound limits – Broadcast 1 megabit – Multicast 1 megabit for RJ45 interfaces – 8 megabit for GBIC or FX interfaces

Network Level	Requirements
Level 2 only	Level 2-only switches have the following configuration: • Uplink inbound limits: None • Level 2 Nodes: Inbound limits: – Broadcast 20 megabit – Multicast 20 megabit • Level 2 Nodes: Inbound prioritization: – CDA packets given priority
Mixed Level 1 and Level 2	Mixed Level 1 and Level 2 configuration have the following configuration: • Uplink inbound limits: – Broadcast 1 megabit – Multicast 1 megabit for RJ45 interfaces – 8 megabit for GBIC or FX interfaces • Level 1 Nodes: Inbound prioritization: – CDA packets given priority • Level 2 Nodes: Inbound limits: – Broadcast 1 megabit – Multicast 1 megabit
Split Level 1 and Level 2	Split Level 1 and Level 2 configuration have the following configuration: • Uplink inbound prioritization: – CDA packets given priority • Level 1 Nodes: Inbound prioritization: – CDA packets given priority • Level 1 Nodes: Inbound filtering • Level 2 Nodes: Inbound limits: – Broadcast 20 megabit – Multicast 20 megabit

Cisco switch and port options

After installing the redundant pair of switches, you will need to 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 Driver package is installed, configure the switch and port options as listed in Table 9-3. Additionally, the configuration files contain Quality of Service parameters that are attached to the ports.

Table 9-3 Cisco switch options

Option Types	Available Options
Switch options	NE-SW224S (2960-24TC[1])
	NE-SW248S (2960-48TC[1])
	NE-SW248G (Cisco 2950G-48[1])
	NE-SW224G (Cisco 2950G-24[1])
	NE-SW312G (Cisco 3550-12G)
	NE-SW312S (Cisco 3750G-12S)
	NE-SW324F (Cisco 3550-24-FX)
	NE-SW324S (Cisco 3560-24TS)
	NE-SW512C (Cisco 2955C-12)
	Honeywell Control Firewall 9
Port configuration options	Number of uplink ports
	Number of full duplex auto speed FTEB ports
	Number of full duplex 100 Megabit ports
	Whether the switch ports have VLAN101 configured.
	Level 1 only, Level 2 only, or Level 1/Level 2 split

[1] The 2960-24TC and 2960-48TC replace the 2950G-24 and the 2950G-48.

Configuration order for switch ports

The specific configuration file you choose defines your 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.

Table 9-4 Cisco switch and port configuration

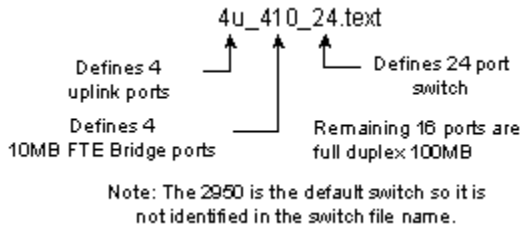
Configuration Order	Port Type	Spanning Tree	Status	Duplex	Speed
1st	Uplink ports	Uplink fast	Enable	Full	100 Mbps
2nd	FTE Bridge ports	Fast	Enable	Full	Auto
3rd	FTE	Fast	Enable	Full	100 Mbps

Switch configuration examples

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

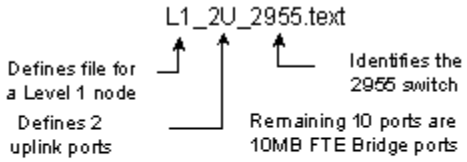
4u_410_24 switch configuration file

This file for the Cisco 2950-24 switch configures 4 uplink ports, 4 FTE Bridge ports and 16 FD 100MB ports.



Up-link	**Up-link**	**10 MB**	**10 MB**	**100 MB**	**100 MB**	**100 MB**	**100 MB**	**100 MB**	**100 MB**	**100 MB**	**100 MB**
Up-link	**Up-link**	**10 MB**	**10 MB**	**100 MB**	**100 MB**	**100 MB**	**100 MB**	**100 MB**	**100 MB**	**100 MB**	**100 MB**

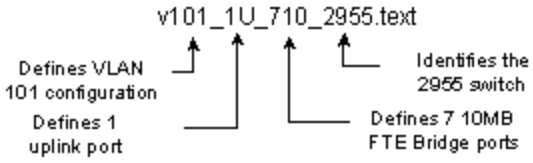
Cisco 2955-12 switch: Level 1, 2 uplink ports, 10 10MB FTE Bridge ports



Note: All 2955 switches have 12 ports so the number of ports is not identified in the switch file name. All ports configured in level 1 switch files are 10 MB FTE Bridge ports except for uplink ports.

Up-link	**10 MB**	**10 MB**	**10 MB**	**10 MB**	**10 MB**
Up-link	**10 MB**	**10 MB**	**10 MB**	**10 MB**	**10 MB**

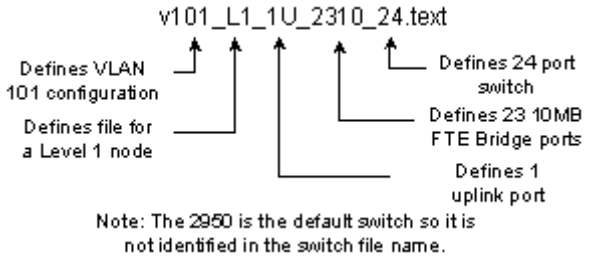
Cisco 2955-12 switch: V101 configured, 1 uplink port, 7 10 MB FTE Bridge ports, 4 FD 100 MB ports



Note: All 2955 switches have 12 ports so the number of ports is not identified in the switch file name.

Up-link	**10 MB**	**10 MB**	**10 MB**	**100 MB**	**100 MB**
10 MB	**10 MB**	**10 MB**	**10 MB**	**100 MB**	**100 MB**

Cisco 2950-12 switch: V101 configured, Level 1, 1 uplink port, 23 10 MB FTE Bridge ports



Up-link	**10 MB**	**10 MB**	**10 MB**	**10 MB**	**10 MB**	**10 MB**	**10 MB**	**10 MB**	**10 MB**	**10 MB**	**10 MB**
10 MB	**10 MB**	**10 MB**	**10 MB**	**10 MB**	**10 MB**	**10 MB**	**10 MB**	**10 MB**	**10 MB**	**10 MB**	**10 MB**

Details for switch configuration files

Table 9-5 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 should be used.

Table 9-5 Switch configuration files

File name	Level	Switch Type	No. of uplinks	No. of 10 MB FTEBs	No. of FD 100 MBs	VLAN101 configured
L1_1u_2310_24	1	2950-24	1	23	0	No
L1_1u_2310_2960_24	1	2960-24	1	23	0	No
L1_1u_2955	1	2955C-12	1	11	0	No
L1_1u_4710	1	2950-48	1	47	0	No
L1_1u_4710_2960	1	2960-48	1	47	0	No
L1_2u_2210_24	1	2950-24	2	22	0	No
L1_2u_2210_2960_24	1	2960-24	2	22	0	No
L1_2u_2955	1	2955C-12	2	10	0	No
v101_L1_1u_2310_24	1	2950-24	1	23	0	Yes
V101_L1_1u_2310_2960_24	1	2960-24	1	23	0	Yes

File name	Level	Switch Type	No. of uplinks	No. of 10 MB FTEBs	No. of FD 100 MBs	VLAN101 configured
v101_L1_1u_2955	1	2955C-12	1	11	0	Yes
v101_L1_1u_4710	1	2950-48	1	47	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
V101_L1_2u_2210_2960_24	1	2960-24	2	22	0	Yes
v101_L1_2u_2955	1	2955C-12	2	10	0	Yes
12u_24	2	2950-24	12	0	12	No
12u_2960_24	2	2960-24	12	0	12	No
12u_3560_24	2	3560-24	12	0	12	No
24u	2	2950-48	24	0	24	No
24u_2960	2	2960-24	24	0	0	No
2u	2	2950-48	2	0	46	No
2u_24	2	2950-24	2	0	22	No
2u_2960	2	2960-48	2	0	46	No
2u_2960_24	2	2960-24	2	0	22	No
2u_3560_24	2	3560-24	2	0	22	No
4u	2	2950-48	4	0	44	No
4u_1610_2960	2	2960-48	4	16	28	No
4u_24	2	2950-24	4	0	20	No
4u_2960	2	2960-48	4	0	44	No
4u_2960_24	2	2960-24	4	0	20	No
4u_3560_24	2	3560-24	4	0	20	No
4u_410_2960	2	2960-48	4	4	40	No
4u_810_2960	2	2960-48	4	8	36	No
fte_3550_cnfg	2	3550-12	12	0	0	No
Fte_3750_cnfg	2	3750-12	12	0	0	No
v101_12u_24	2	2950-24	12	0	12	Yes
V101_12u_2960_24	2	2960-24	12	0	12	Yes
V101_12u_3560_24	2	3560-24	12	0	12	Yes
V101_24u	2	2950-48	24	0	24	Yes

File name	Level	Switch Type	No. of uplinks	No. of 10 MB FTEBs	No. of FD 100 MBs	VLAN101 configured
V101_24u_2960	2	2960-48	24	0	24	Yes
v101_2u	2	2950-48	2	0	46	Yes
v101_2u_24	2	2950-24	2	0	22	Yes
V101_2u_2960	2	2960-48	2	0	46	Yes
V101_2u_2960_24	2	2960-24	2	0	22	Yes
V101_2u_3560_24	2	3560-24	2	0	22	Yes
v101_4u	2	2950-48	4	0	44	Yes
v101_4u_24	2	2950-24	4	0	20	Yes
V101_4u_2960	2	2960-48	4	0	44	Yes
V101_4u_2960_24	2	2960-24	4	0	20	Yes
V101_4u_3560_24	2	3560-24	4	0	20	Yes
v101_fte_3550_cnfg	2	3550-12	12	0	0	Yes
V101_fte_3750_cnfg	2	3750-12	12	0	0	Yes
1u_710_2955	1 & 2	2955C-12	1	7	4	No
2u_1010_split_2960_24	1 & 2	2960-24	2	10	12	No
2u_1010_split_2960_24	1 & 2	2960-24	2	10	12	No
2u_1010_split_3560_24	1 & 2	3560-24	2	10	12	No
4u_1610	1 & 2	2950-48	4	16	28	No
4u_1610_24	1 & 2	2950-24	4	16	4	No
4u_1610_2960_24	1 & 2	2960-24	4	16	4	No
4u_2110_split_2960	1 & 2	2960-48	4	21	23	No
4u_2110_split_2960	1 & 2	2960-24	4	21	23	No
4u_410	1 & 2	2950-48	4	4	40	No
4u_410_24	1 & 2	2950-24	4	4	16	No
4u_410_2960_24	1 & 2	2960-24	4	4	16	No
4u_810	1 & 2	2950-48	4	8	36	No
4u_810_24	1 & 2	2950-24	4	8	12	No
4u_810_2960_24	1 & 2	2960-24	4	8	12	No
V101_1010_2960_24	1 & 2	2960-24	0	10	14	Yes
v101_1u_710_2955	1 & 2	2955C-12	1	7	4	Yes
V101_2u_1010_3560_24	1 & 2	3560-24	2	10	12	Yes

File name	Level	Switch Type	No. of uplinks	No. of 10 MB FTEBs	No. of FD 100 MBs	VLAN101 configured
v101_4u_1610	1 & 2	2950-48	4	16	28	Yes
v101_4u_1610_24	1 & 2	2950-24	4	16	4	Yes
V101_4u_1610_2960	1 & 2	2960-48	4	16	28	Yes
V101_4u_1610_2960_24	1 & 2	2960-24	4	16	4	Yes
v101_4u_410	1 & 2	2950-48	4	4	40	Yes
v101_4u_410_24	1 & 2	2950-24	4	4	20	Yes
V101_4u_410_2960	1 & 2	2960-48	4	4	40	Yes
V101_4u_410_2960_24	1 & 2	2960-24	4	4	16	Yes
v101_4u_810	1 & 2	2950-48	4	8	36	Yes
v101_4u_810_24	1 & 2	2950-24	4	8	12	Yes
V101_4u_810_2960	1 & 2	2960-48	4	8	36	Yes
V101_4u_810_2960_24	1 & 2	2960-24	4	8	12	Yes
V101_stack[1]	1 & 2	3750-24 (up to 9)	0	0	0	Yes
V101-4u_2110_2960	1 & 2	2960-48	4	21	23	Yes

1 This file must be modified for each switch in the stack. See "**Modifying the stacked switch configuration files**" on page 85 for details.

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 switch's command line interface and the correct switch startup configuration file.

Before you begin

Before beginning the procedures in this section, verify the following:

✓	Task
	You have an RS-232 cable configured, as required by the switch vendor, to connect the computer's serial port to the switch's comm port.
	Have HyperTerminal configured on the computer to be used as the interface to the switch.
	Have reviewed the specific vendor's switch user guide, if necessary.

Passwords and names for switch access and configuration

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

Name	Description	Example Used in This Document
Virtual Terminal Password	Password used to protect access to the router over a network interface.	*FTE4*
FTP Server Username	FTP Server username 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*
Enable Secret	Password used to protect 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*

Tasks for configuring a Cisco switch

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

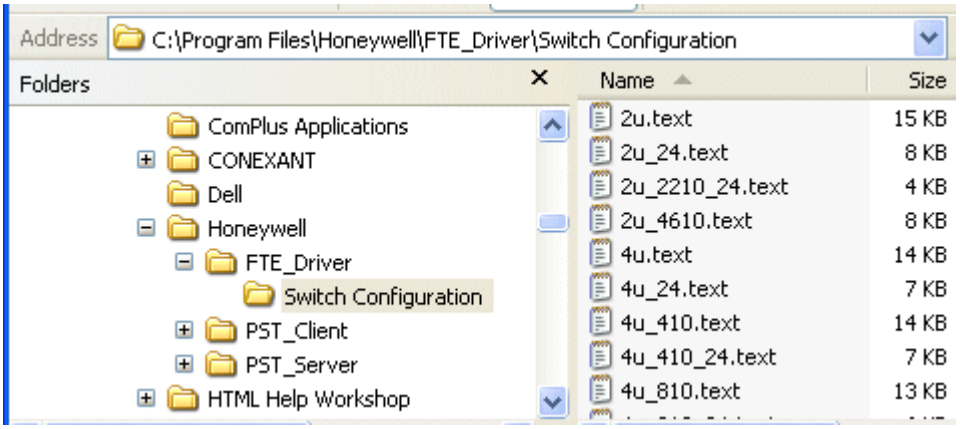
Table 9-6 Cisco switch configuration tasks

✓	Task
	Connect to the switch. See “Connecting locally to the switch” on page 103
	Verify the switches have the IOS version qualified by Honeywell as listed in the SCN for your release. **Note**: If the version is not the same as that listed in the SCN, contact Honeywell Network Services for the procedure to upgrade the IOS.
	Configure the switch. See “Configuring switch interface options” on page 104.
	Load the switch configuration file. See “Loading the switch configuration file” on page 111.

Accessing switch configuration files

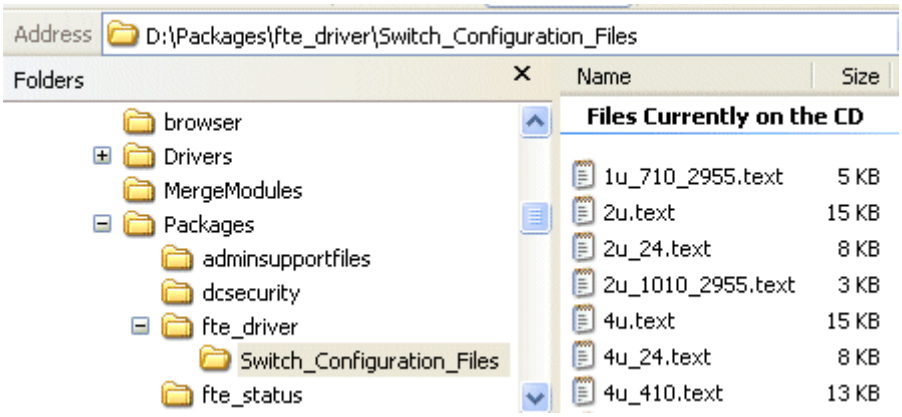
Switch configuration files are packaged with the FTE Driver and are copied to the following location when you run the FTE Driver installation package.

C:\Program Files\Honeywell\FTE_Driver\Switch Configuration



If you have not yet installed FTE, you may access switch configuration files from the Experion Application DVD at the following location:

Media Drive:\Packages\FTE_Driver\Switch_Configuration_Files



Using the Cisco Command Line Interface (CLI)

After connecting to the switch, you can to 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 table lists the conventions used in the switch configuration procedures and examples.

Table 9-7 Conventions used to convey instructions and information

`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#`**`config t`**
`Enter configuration commands, one per line. End with CNTL/Z.`
`Cisco_FTE4(config)#int vlan1`
	Values that are entered by the user are in **bold**.

`Enter host name [Switch]:` ***`Cisco_FTE4`***	Arguments for which the user supplies the values are in ***bold italic.***
`Destination filename [config.text]?<ENTER>` `Writing config.text !!!!`	Nonprinting characters, such as passwords or Enter key, are in angle brackets (< >).

Connecting locally to the switch

Use the following procedure to connect to the switch and start HyperTerminal.

ATTENTION

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

Step	Action
1	Connect the RS-232 cable to the Switch's Comm Port and the computer's serial port.
2	Click **Start > Programs > Accessories > Communications > HyperTerminal**.
3	From the **Connection Description** dialog box, type a name that describes the connection in the **Name** box and then click **OK.**
4	In the **Icon** box, click the appropriate icon, and then click **OK.**
5	From the **Connect To** dialog box, select the serial port being used by the computer in Connect Using box and then click **OK**.
6	From the **Connect To** dialog, select the serial port being used by the computer and click **OK.**
7	From the **Properties** page configure the following Port Settings: • Bits per second: 9600 • Data Bits: 8 • Parity: NONE • Stop bits: 1 • Flow control: Xon/Xoff
8	Click **OK.**
9	Power up the switch and go to the next procedure.

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.

Step	Action
	**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**. Supply your own 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 your own host name and password when asked to do so.

Step	Action
3	When the following display appears, type all values that appear in **bold**. Supply 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 displays 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**.

Step	Action

```
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
```

Step	Action
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 is the end of 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.
```

9	Use the enable command and the enable secret you previously established: ***Cisco_FTE1*** is used in the following example. Type all values that appear in **bold**. Supply your own values for the text that appears in ***bold italic***.

```
Press RETURN to get started!<ENTER>
Cisco_FTE4>enable
Password:Cisco_FTE1
```

10	If VLAN101 is to be used, initialize VLAN 101 by performing these additional steps: • Type **vlan101** • Type **exit** • Type **exit** Otherwise, go to the next step.

Step	Action
11	To enable Telnet and FTP, use one of the following commands: • To configure vlan1, type **int vlan1**, or • To configure vlan101, type **int vlan101**: Type all values that appear in **bold**. Supply your own values for the text that appears in ***bold italic***.

```
Cisco_FTE4#config t
Enter configuration commands, one per line.  End with CNTL/Z.
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**. Supply 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 rights to allow FTP access. You can then archive and restore configurations using telnet and the FTP server.

13	You need a user name and password for your FTP Server. The following are used as the examples in the switch displays: ***ps_user -*** example user name ***ps_user local –*** example password ***FTE4 –*** example virtual terminal password Type all values that appear in **bold**. Supply 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
```

Step	Action
14	The switch generates SNMP traps when the switch reboots or has a link go up or go down. The switch must have a target IP address for the SNMP traps, which will be the IP address of the server that is running the EPKS System. Systems with redundant servers need to have both server IP addresses configured in the switches for SNMP. You should 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**. Supply 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 your system has redundant servers, repeat the #**snmp-server host *10.1.4.16 FTE* snmp** command using the redundant server IP address (***10.1.4.16*** – is used as an example for the redundant server IP address).
16	To enable SNMP reads of the switch statistics, type: Snmp-server community ***public*** RO **Note**: ***Public*** is the community name default as configured in the Experion SPS. This is **not** a secure name and should have already been changed using the System Definition tool from Configuration Studio.

ATTENTION – NTP Time Server

The Windows SNTP service does not provide the proper protocol for NTP that the switch expects. For this reason, you must configure an NTP timeserver in order to synchronize time with other switches and network nodes. Examples of NTP Time Servers:

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

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

Step	Action
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**. Supply 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**. Supply 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 should be the vlan used if it is different from *101* Type all values that appear in **bold**. Supply 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 cda-policy
Cisco_FTE4(config)#srr-queue bandwidth share 1 2 3 4
```

20	Type **exit**. 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.

Using VLAN101 switch configuration files

If your system requires you to disable VLAN1 in the switches, you will need to use the alternate switch configuration files that are preceded with *V101_*. For example, instead of using *4u.text*, you would use the *V101_4u.text* file. See Table 9-5 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.

Loading the switch configuration file

The following procedure uses Hyperterm's Xmodem file transfer utility to transfer the correct switch configuration file from the installation media to the switch. After downloading the switch configuration file, you will write the configuration back to the switch memory.

Press Enter after typing each value.

TIP

If you are not familiar with Xmodem, read Hyperterm's help and try a practice transfer before initiating the transfer in the switch. Read steps 1 through 6 in the following procedure before you begin.

Step	Action
1	Review Table 9-5 to determine the most appropriate switch configuration file for your system.
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>
```

Step	Action
3	Initiate the transfer in Hyperterm and choose the appropriate switch configuration file: • From the Hyperterm menu bar, select **Transfer > Send File**. • Select Browse and navigate to the **Switch Configuration** folder in the following location: – *C:\Program Files\Honeywell\FTE_Driver\, or* – *Media Drive:\Packages\FTE_Driver\Switch_Configuration_Files, or* – *Location you saved the files to* • Select the correct switch configuration file for your particular system and click **OPEN**. • Select **Xmodem** under **Protocol**. • Click Send to start the file transfer.
4	If there is an existing file with the same name, type **y** to overwrite the file.

```
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]y
Begin the Xmodem or Xmodem-1K transfer now...
CCCCCCCCCC
```

5	If there is a problem during the transfer, an error message displays by the switch. If this happens, retype the following command and press ENTER:

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

6	The following displays 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 to 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 you 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
```

Step	Action

```
service timestamps log uptime
no service password-encryption
service sequence-numbers
!
hostname Cisco_FTE4
!
enable secret 5 $1$JIQ6$IJ3nKv2oS2zCJZihoHEKl/
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
```

Step	Action

```
 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
```

Step	Action

	`line vty 0 4`
	` password FTE1`
	` login`
	`line vty 5 15`
	` password FTE1`
	` login`
	`!`
	`end`
	
	`Cisco_FTE4#`

10	This is the end of the switch configuration. If you would like to archive the configuration file for future use, see Section 9.8.

9.8 Saving and modifying Cisco switch configuration files

Use the procedures in this section to save, modify and restore the switch configuration files. Following are the circumstances in which you may need to perform these tasks:

- A switch fails and you need to reload the switch configuration file.
- You add a new node type to the network
- You want to use an existing configuration file on another switch.

Downloading the switch configuration file (optional)

Use the following procedure to save a file containing the switch options you configured. This makes it easier to reconfigure the switch in case of a switch failure. Press Enter after entering each value.

Step	Action
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 asked to enter a password. Type the virtual terminal password you previously configured for the switch and press Enter. ***FTE4*** is used in the following example.

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

Step	Action
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**. Supply 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. Type all values that appear in **bold**.

```
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 your switch configuration files to this location.

TIP

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

9.9 Installing and configuring Nortel switches

After installing the redundant pair of switches in your specific furniture, you will need to configure the switches for FTE. Perform all procedures in this section regardless of the type of furniture in which you installed the switches.

Before you begin

Before beginning the procedures in this section, verify the following:

✓	Task
	You have a UL-listed RS-232 cable configured as required by the switch vendor to connect the computer's serial port to the switch's comm port.
	Have HyperTerminal configured on the computer to be used as the interface to the Switch Configuration menu.
	Have reviewed the specific vendor switch user guide.

Tasks for installing and configuring a Nortel switch

Table 9-8 Nortel Switch Installation and Configuration Tasks

✓	Task
	Be aware of FTE cable requirements
	Install switches
	Configure switches
	Install additional switch components, if necessary
	Disable Snooping and Spanning Tree on Nortel switch
	Configure the connection speed for switch ports
	Connect crossover cables

Disable Snooping and Spanning Tree on Nortel switch

Use the following procedure to disable IGMP Snooping and Spanning Tree on a Nortel (BayStack) Switch. Refer also to your BayStack Series Switch manual for details on the switch menus.

ATTENTION

To minimize the opportunity for IP Multicast problems, ALL switches on ALL systems, regardless of software revision, should be configured to disable snooping.

CAUTION

Enabling Spanning Tree on a Nortel switch directly conflicts with FTE and may cause packet loss, broadcast storms, and extended recovery time from faults. Spanning tree is unnecessary when the FTE Community is properly connected.

Step	Action
1	Connect the RS-232 cable to the Switch's Comm Port and the computer's serial port.
2	Click **Start > Programs > Accessories > Communications > HyperTerminal**.
3	From the **Connection Description** dialog box, type a name that describes the connection in the **Name** box and then click **OK.**
4	In the **Icon** box, click the appropriate icon, and then click **OK.**
5	From the **Connect To** dialog box, select the serial port being used by the computer in Connect Using box and then click **OK**.
6	From the **Connect To** dialog, select the serial port being used by the computer and click **OK.**
7	From the **Properties** page make the following Port Settings: • Bits per second: 9600 • Data Bits: 8 • Parity: NONE • Stop bits: 1 • Flow control: Xon/Xoff

Step	Action
8	Verify the connection between the computer and the switch.
	**TIP** See the section on Using the Console Interface in your Nortel Switch manual for additional information on using the Console Interface menus.
9	Press **CTRL+Y** to display the switch's control interface main menu.
10	Select **Switch Configuration** from the main menu.
11	Select **IGMP Configuration** from the **Switch Configuration Menu**.
12	Select the **Snooping** option from the **IGMP Configuration**.
13	Highlight **Enabled** and press the space bar to set the **Snooping** option to **Disabled**.
14	Press **Ctrl + C** to return to the Main Menu.
15	Select **Spanning Tree Configuration** from the Main Menu.
16	Select **Spanning Tree Port Configuration** from the **Spanning Tree Configuration Menu**.
17	Use the space bar to display the **Disabled** option.
18	Highlight the **Disabled** option and press Return or Enter to set the **Spanning Tree** option.
19	Press **Ctrl + C** to return to the Main Menu.
20	Check the system to ensure all communications are working correctly. If not, correct the problem before continuing.
21	***Save configuration changes and repeat the procedure for the second switch.***

Configure the connection speed for switch ports

By default, the switch packaged with FTE has auto negotiation enabled. In the case of a fault recovery, however, communications may slow down while the port connection speed is being detected, and cause collisions. Manually setting the port connection speed for the switch and the FTE node ports to be compatible improves performance and decreases the likelihood of communication collisions. Perform this procedure with the RS-232 cable still connected to the Switch's Comm Port and the computer's serial port.

CAUTION

Keeping the switch set to auto negotiate may cause communication traffic slow downs that could result in excessive Ethernet collisions.

Step	Action
	**TIP** See the section on Using the Console Interface in your Nortel Switch manual for additional information on using the Console Interface menus.
1	Press **CTRL+Y** to display the switch's control interface main menu.
2	Select **Switch Configuration** from the main menu.
3	Select **Port Configuration** from the **Switch Configuration Menu**.
4	Highlight the switch port that is being configured.
5	Use the space bar to display the **Autonegotiation** option.
6	Highlight the **Disabled** option and press Return or Enter to set the **Autonegotiation** option.
7	Use the space bar to display the **Speed Duplex** option.
8	Highlight the port connection speed option that is compatible with the FTE node ports.
9	Press Return or Enter to set the **Speed Duplex** option.
10	Press Ctrl –C to return to the **Main Menu**.
11	Close the Main Menu.
12	Check the system to ensure all communications are working correctly. If not, correct the problem before continuing.
13	***Save configuration changes and repeat the procedure for all switch ports being used for FTE.***

Connect crossover cables

Use the following procedure to connect the crossover cable at the highest level of switches.

WARNING

Only the highest level of redundant switches in the LAN should be interconnected using the crossover cable or a router. Multiple crossover cables will cause path loops and take down your network.

Step	Action
1	Connect one end of the crossover cable to one of the configured uplink port connectors on the front panel of the switch in the *Yellow* Tree.
2	Connect the other end of the crossover cable to one of the configured uplink port connectors on the front panel of the switch in the *Green* Tree.

9.10 Updating the Honeywell Control Firewall firmware

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

Firewall devices

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

- Control microprocessor
- Filter FPGA

Determining necessity of firmware update

Do not update the firmware image on your Honeywell Control Firewall until you have verified it is necessary by doing the following:

- Review the SCN for your release to determine the required Honeywell Control Firewall firmware image for your release.
- Determine your current firmware revision by viewing the System Status detail display for the Honeywell Control Firewall.

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 be sure there were no data errors.
- When the process is complete, the 9th port LED stops flashing returns to normal operation.

2 The CRC 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 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 resets:

- 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 resets.

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.

Before using the Control Firewall Update Tool

All of the following conditions must be met before you can use this tool:

- The Control Firewall Update Tool package must be installed.
- The FTE 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.

Launch the Control Firewall Update Tool

To launch the tool from Configuration Studio

Step	Action
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

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

10. Troubleshooting Network Issues

10.1 Preventing crosslink errors

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 TCP/IP network binding order to define which interface is *yellow* and which interface is *green*. The interface port connection that is first in the binding order is defined as *yellow* and the interface port connection that is second in the binding order is defined as *green*. This binding order must remain consistent in order to maintain the correct interface port designation for the messages.

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. When the trees are isolated from one another, however, the diagnostic messages should also be isolated – only messages designated as *yellow* should be seen on the *Yellow* tree - only messages designated as *green* should 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.

Potential causes of crosslink errors

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

Table 10-1 Crosslink Errors – Potential Causes

Cause	Examples
Cables are crossed at the node or at the switches.	Cable with the yellow boot is connected to the Switch in the *Yellow* Tree, but it is connected to the second port. Cable with the green boot is connected to the Switch in the *Green* Tree, but it is connected to first port. Connection for first port (cable with yellow boot) is connected to the Switch in the *Green* Tree. Connection for second port (cable with the green boot) is connected to the Switch in the *Yellow* Tree.
Both FTE cables are connected to the same Tree.	Cable with the yellow boot and cable with the green boot are connected to the same switch.
Binding order is “reversed”.	Cable with the yellow boot is connected to the first port and to the Switch in the *Yellow* Tree, but the connection for the first port appears SECOND in the binding order. Cable with the green boot is connected to the second port and to the Switch in the *Green* Tree, but the connection for the second port appears FIRST in the binding order.
FTE Network topology does not follow configuration rules.	Any condition that creates network path loops, such as any of the following: • FTE Network has more than one crossover cable • Multiple connections to an external network • Switches are not in a tree hierarchy

11. Switch and router configuration examples

11.1 Cisco switch and router examples

Cisco 2950 Configuration Example

The following configuration file is an example of 4u_410.text which will configure:

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

```
!
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 igmp snooping
!
spanning-tree extend system-id
!
!
interface FastEthernet0/1
 no ip address
 duplex full
 speed 100
 service-policy input cda_policy
!
interface FastEthernet0/2
 no ip address
 duplex full
 speed 100
 service-policy input cda_policy
!
interface FastEthernet0/3
 no ip address
```

```
 duplex full
 speed 100
 service-policy input cda_policy
!
interface FastEthernet0/4
 no ip address
 duplex full
 speed 100
 service-policy input cda_policy
!
interface FastEthernet0/5
 no ip address
 duplex full
 speed auto
 service-policy input cda_policy
 spanning-tree portfast
!
interface FastEthernet0/6
 no ip address
 duplex full
 speed auto
 service-policy input cda_policy
 spanning-tree portfast
!
interface FastEthernet0/7
 no ip address
 duplex full
 speed auto
 service-policy input cda_policy
 spanning-tree portfast
!
interface FastEthernet0/8
 no ip address
 duplex full
 speed auto
 service-policy input cda_policy
 spanning-tree portfast
!
interface FastEthernet0/9
 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 100.00 100.00
 storm-control action trap
 spanning-tree portfast
!
interface FastEthernet0/10
 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 100.00 100.00
 storm-control action trap
 spanning-tree portfast
!
```

interface FastEthernet0/11 through interface FastEthernet 0/48 are identical to interface FastEthernet0/10

```
!
no 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
!
end
```

Cisco 4xxx series router configuration example

This example shows two FTE communities. Each subnet has 255 total addresses with 15 IP addresses used for the server range. The first community is 10.0.0.0-255 and the second is 10.0.1.0-255. The access lists limit the server range to have unfiltered access, the remaining part of the range to have "established" access and the ports 88 and 389 enabled to all nodes for authentication communication.

```
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service compress-config
!
hostname FTE4006
!
logging console errors
!
vtp mode transparent
!
vlan 101
 name FTE_1
!
vlan 102
!
vlan 103
 name FTE_3
!
vlan 104
 name FTE_4
ip subnet-zero
no ip igmp snooping
ip ftp username ps_user
ip ftp password ps_user local
!
ip multicast-routing
ip multicast multipath
!
!
interface GigabitEthernet1/1
 no snmp trap link-status
!
```

```
interface GigabitEthernet1/2
 no snmp trap link-status
!
interface GigabitEthernet2/1
 no snmp trap link-status
!
interface GigabitEthernet2/2
 no snmp trap link-status
!
interface FastEthernet2/3
 switchport access vlan 101
 switchport mode access
 duplex full
 speed 100
 no snmp trap link-status
!
interface FastEthernet2/4
 switchport access vlan 101
 switchport mode access
 duplex full
 speed 100
 no snmp trap link-status
!
interface FastEthernet2/5
 switchport access vlan 102
 switchport mode access
 duplex full
 speed 100
 no snmp trap link-status
!
interface FastEthernet2/6
 switchport access vlan 102
 switchport mode access
 duplex full
 speed 100
 no snmp trap link-status
!
interface FastEthernet2/7
 switchport access vlan 103
 switchport mode access
 duplex full
 speed 100
 no snmp trap link-status
!
```

Interfaces 9 and greater are other VLAN interfaces than FTE Communities

```
interface Vlan101
 ip address 10.0.0.1 255.255.255.0
 ip access-group 101 out
 no ip proxy-arp
 ip pim dense-mode
!
interface Vlan102
 ip address 10.0.1.1 255.255.255.0
 ip access-group 102 out
 no ip proxy-arp
 ip pim dense-mode
!
ip classless
no ip http server
!
access-list 101 permit tcp 10.0.0.0 0.0.0.255 any established
access-list 101 permit udp host 225.7.4.103 any
access-list 101 permit udp any host 225.7.4.103
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
access-list 101 permit udp any any eq domain
access-list 101 permit udp any any eq 88
access-list 101 permit udp any any eq 389
access-list 102 permit tcp 10.0.1.0 0.0.0.255 any established
access-list 102 permit udp host 225.7.4.103 any
access-list 102 permit udp any host 225.7.4.103
access-list 102 permit ip 10.0.1.0 0.0.0.240 any
access-list 102 permit ip any 10.0.1.0 0.0.0.240
access-list 102 permit udp any any eq domain
access-list 102 permit udp any any eq 88
access-list 102 permit udp any any eq 389
```

11.2 Cisco router configuration statements

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

Access Control Lists

Cisco uses an Access Control List (ACL) to describe what should pass and what should 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.

Cisco 3560 access list for protecting Safety Manager or third-party safety controllers

A level of protection can be afforded to 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 a access-group that is attached to the crosslink interface of the split switch on the L1 half. The configuration file would contain:

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 could be modified to substitute the above for the access-list 130 in the file before downloading to the switch

Then for a split switch the L1 uplink interface is Fast Ethernet 0/13 so the configuration file would contain:

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 would not be needed due to the strict filtering only allowing server traffic through.

11.3 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 0xFFFFFFF8 (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 0xFFFFFFC0 (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 0xFFFFFC00 (255.255.252.0)
- L1 Node Netmask:
- Must ignore all unique L2 and L1 address bits = 0xFF000000 = 255.0.0.0

11.4 Stacked Switch Configuration Examples

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
```

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
```