Honeywell

**Experion**

# Fault Tolerant Ethernet
# Overview and Implementation
# Guide

EP-DSX243
R210
09/04

# 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 Overview and Implementation Guide - **FE02** | EP-DSX243 | 210 | 09/04 |

## 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.<br>Industry Solutions | 1-800-343-0228<br>1-800-525-7439<br>1-800-822-7673 | Sales<br>Service<br>Technical Support |
| Asia Pacific | Honeywell Asia Pacific Inc.<br>Hong Kong | (852) 23 31 9133 | |
| Europe | Honeywell PACE<br>Brussels, Belgium | [32-2] 728-2711 | |
| Latin America | Honeywell International Inc.<br>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.<br><br>**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.<br><br>**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

**Contents**

# 1. Introduction

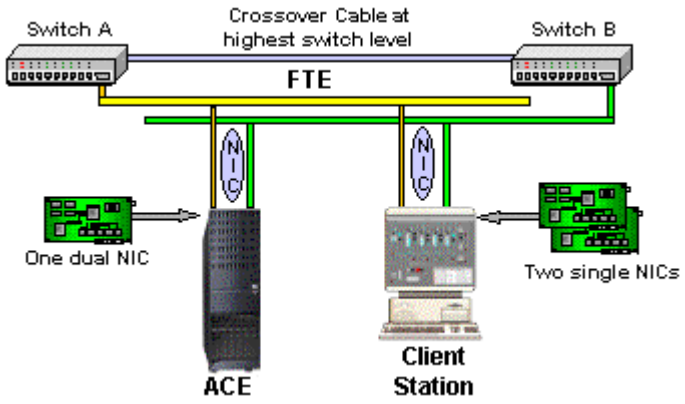
## 1.1 Fault Tolerant Ethernet (FTE) Functional Overview

### 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 not only fault tolerance, but fast response, 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**



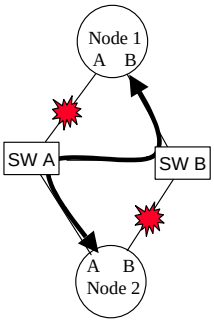
### Communication between FTE nodes

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 1-1 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).

## 1.2 About this Document

### Scope

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 installation is familiar with networking fundamentals. Table 1-4 contains a list of additional documents from third-party vendors that may be useful.

### 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 1-2 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 |
| 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 1-3 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 collection of FTE and non-FTE nodes within a community. |
| 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.<br>• Tree A is *Yellow*<br>• 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 1-4 References for FTE Components**

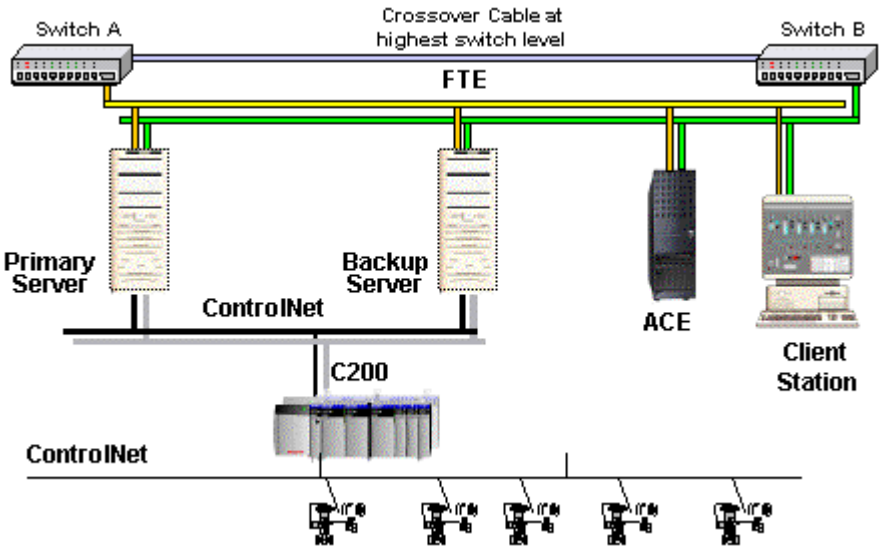
| For more information on . . . | See this reference . . . |
|---|---|
| Cisco switches | For all user guides, go to<br>http://www.cisco.com/<br>and search for "Cisco Catalyst" |
| Nortel switches | For all user guides, go to<br>http://www.nortelnetworks.com/<br>and search for "BayStack 450" |
| Intel network cards | For all user guides, go to<br>http://support.intel.com/support/network/adapter/<br>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*<br>**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* |

# 1.3 FTE Networking Concepts

### 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 or by connecting the switch pair to a single router. 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

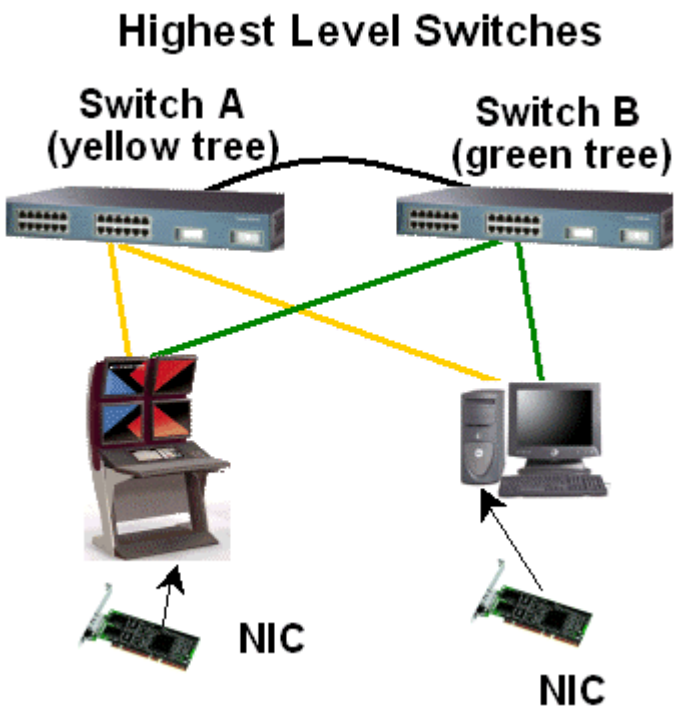
An FTE Community is a group of FTE and non-FTE nodes within the same broadcast domain. FTE nodes are dually connected nodes that have fault tolerant communication coverage using FTE test messages. Non-FTE nodes are singly or dually connected nodes that do not have FTE. Honeywell does not recommend multiple FTE communities within 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 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 will be 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.

# 1.4 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.

### Role of Honeywell Network Services

Honeywell's network services groups can design, configure and implement security firewalls for your FTE network. They can also provide consulting, installation, and support services for other network components, and certify additional PCs and network equipment that may be required in an FTE network. Contact the Solution Support Center at 1-800-822-7673 to discuss networking services options.

### Tasks for planning an FTE network

Consider the following network requirements before installing your FTE network.

**Table 1-5 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. Planning a Honeywell FTE Network

## 2.1 FTE Network Infrastructure

### Introduction

An FTE network is comprised of a variety of node types and networking components. This section describes the considerations and requirements for connecting and configuring these elements 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 2.2 through 2.5 of this document provide further details on these levels, including specific network best practices for each level.

**Table 2-1 FTE Network Levels**

| Level | Description of Nodes in this Level | Go to |
|---|---|---|
| Level 1 | Real Time Control (controllers and IO) | Section 2.2 |
| Level 2 | Supervisory Control, Operator HMI (HMI, and Supervisory Controllers) | Section 2.3 |
| Level 3 | Advanced Control and Advance Applications (Non Critical Control Applications) | Section 2.4 |
| Level 4 | Plant Level Applications (MES and MRP) | Section 2.5 |

### 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 singly attached or are dually attached but do not run FTE may also be members of the FTE community. Honeywell does not recommend multiple FTE communities in the same broadcast domain.

### Maximum nodes within an FTE Community

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

**Table 2-2 Singly & Dually Connected Nodes in FTE Community**

| Singly or Dually Connected | Characteristics | Network View |
|---|---|---|
| Dually 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. | Will be seen as one FTE node when it shares the same multicast address. If the node is outside the multicast scope, it will be seen as two non-FTE nodes. |
| Singly connected Ethernet nodes | Node can be communicated with. | Will be 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.

### Best practices architecture

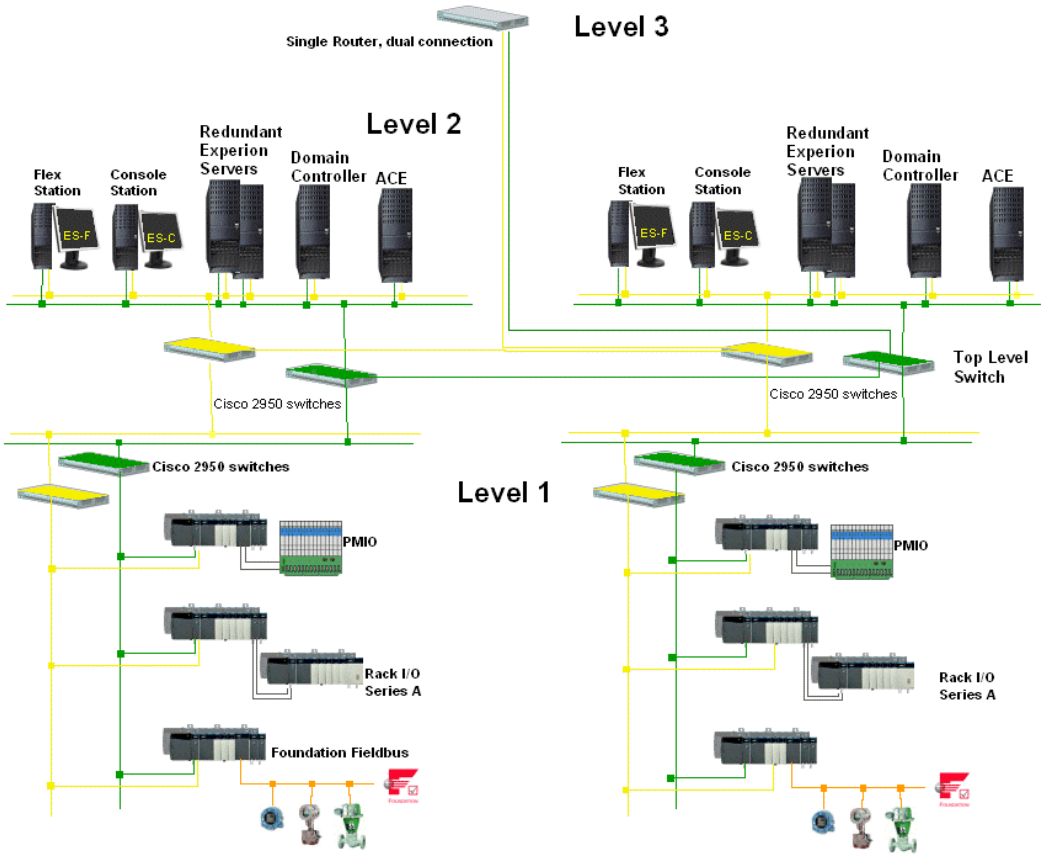
The topology diagrams in this document represent Honeywell's recommended best practice for installation of a large system. While variations of the architecture are possible, the topology examples represent the highest level of security and reliability. The emphasis is on isolating critical areas of function 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.

### Using a single router with dual connections

If you are using a router, the highest level switches are inter-connected using dual connections to a single router as follows:

- Create a Virtual Local Area Network (VLAN) in the router that has two interfaces.
- Verify the VLAN number in the router matches the VLAN in the FTE switches.
- Connect the highest level FTE switch in the yellow tree to one interface.
- Connect the highest level FTE switch in the green tree to the other interface.
- Do not attach a crossover cable between the top level switches as the two ports VLAN and the dual connections act as a crossover cable.



### 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 2-3 FTE Critical Configuration Items**

| | Requirement | For more information see . . . |
|---|---|---|
| ✓ | Level 1 nodes must not have a default router configured. | Section 2.2 & FTE Bridge Installation documents |
| ✓ | Multiple communities on a single subnet are not recommended. | Section 2.2 |
| ✓ | Server IP addresses are in a range separate from other nodes. | Section 2.3 |
| ✓ | Routers must have the access lists added for proper filtering of traffic to Level 2. | Section 2.3 |
| ✓ | A firewall between Level 4 and Level 3 is critical to the security of the control nodes on Level 2 and Level 1. | Section 2.5 |
| ✓ | Private IP addresses should be used where possible with NAT to corporate networks. | Section 3.2 |
| ✓ | Level 1 addresses are in a subnet separate from other Level 2 nodes. | Section 3.4 |
| ✓ | Level 1 addresses must be in a separate, reusable range when communication with Level 4 is necessary. | Section 3.4 |
| ✓ | Level 2 nodes that communicate with Level 1 nodes must have the “route add” configured. | Section 3.4 |
| ✓ | Router VLANs where FTE communities are connected MUST have no ip proxy-arp configured. | Section 3.4 |
| ✓ | Switches are configured with the Honeywell configuration files. | Sections 4.2 & 4.3 |
| ✓ | Experion PKS nodes and switch/router uplinks (downlinks) must be connected to appropriately configured interface ports on the switches. | Sections 4.2 & 4.3 |

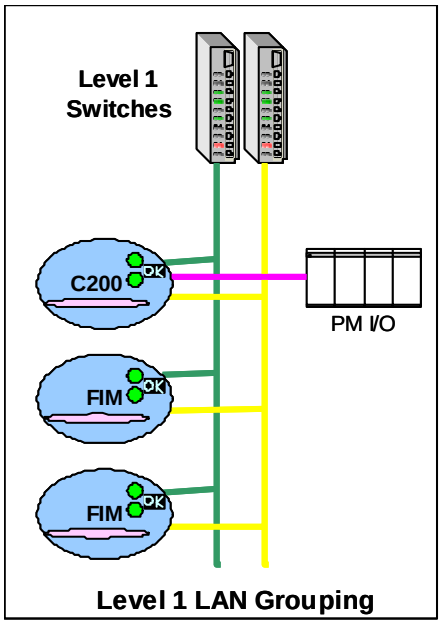
## 2.2 Level 1

### Description

Level 1 nodes are the heart of the control system. This network segment contains controller nodes and the FIM nodes, which connect to the FTE network through the FTEB.

### Level 1 LAN grouping

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



Level 1 LAN Grouping

**Citizenship:**

- Level 1 Cisco 2950 Switches
- Controllers
- Fieldbus Interface Modules

**Level 1 Switches:**

- Provide point-to-point connectivity for FTE devices in cabinet.
- Provide high reliability configuration
  - Are always redundant.
  - Pre-configure CDA traffic in high priority switch queue.
  - Pre-configure other traffic in low priority switch queue.
- Provide additional switch attributes:
  - One megabit broadcast storm
  - One megabit multicast policing on 100 base T uplinks
  - Eight megabit multicast policing on GBIC uplinks

### Level 1 best practices

The Level 1 best practice is to place Level 1 nodes on a separate switch pair from the other levels. This allows critical peer-to-peer traffic to flow only locally on the switch's backplane. 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 switches. Because this level includes controller nodes, the critical control traffic must have adequate bandwidth. Ensuring sufficient bandwidth is described in the next section, "Complying with Level 1 best practices."

### Complying with Level 1 best practices

First, the 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 output queue must be configured in the switches to ensure control traffic precedes lower priority traffic as follows:

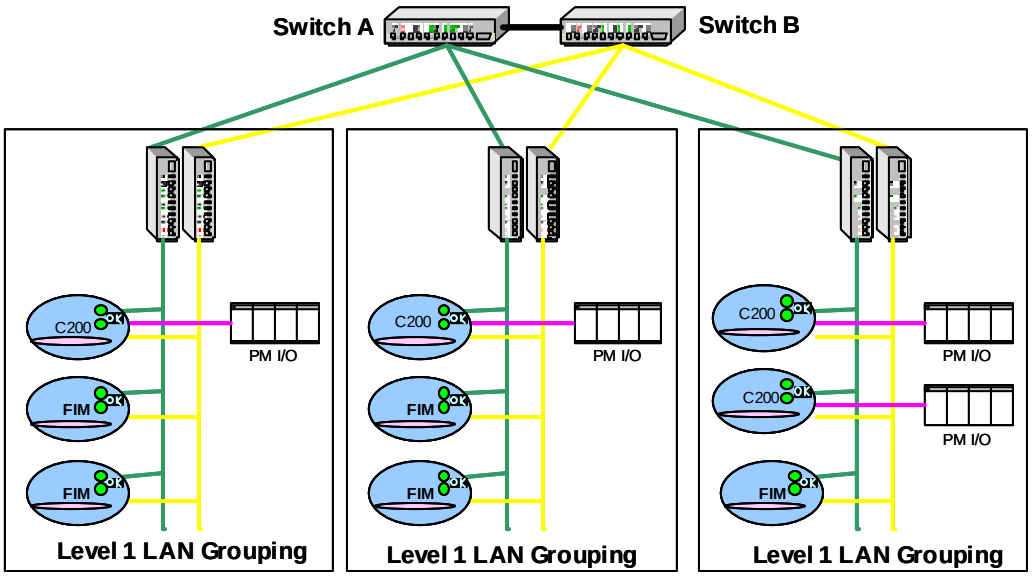
- Control traffic is routed to the highest priority queue.
- Display traffic is routed to the second level priority queue.
- Any remaining traffic is routed to the lowest priority queue.

Second, the IP address for the embedded nodes, FTE Bridge for example, has special characteristics. Honeywell recommends that the range of the address be in a separate address space from the rest of the Level 2 address space that is defined by the subnet mask set in each node. By doing this, only nodes on Level 2 that have a "route add" configured to this address space can communicate with the embedded Level 1 nodes. The Level 1 nodes will not be visible to Level 2 nodes without the added route, nor will they be visible to any Level 3 nodes. Section 3, "Use of IP Addresses in an FTE Network" discusses the IP ranges to be used for embedded nodes and Level 2 nodes.

### Connection of Level 1 LAN groupings

The following diagram shows several Level 1 LAN groupings connected with a second layer of switches. The main purpose of this configuration is to allow critical peer-to-peer traffic to flow only locally.

**Switches to Connect Level 1 LAN Groupings**




**Citizenship:**

- Cisco 2950 Switches
- Level 1 LAN groupings

**Cisco 2950 Switches:**

- Provide connectivity for Level 1 groupings
- Provide 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 2950 faults impact inter-cabinet traffic only
- Provide additional switch attributes:
  - One megabit broadcast storm
  - One megabit multicast policing on 100 base T uplinks
  - Eight megabit multicast policing on GBIC uplinks

### Connection of Level 1 nodes that intercommunicate using Level 2 switches

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 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 will be tagged with the highest priority at the ingress.
- The output queue to the destination Level 1 node will send 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, the Level 2 switches are configured to have storm protection on the interfaces where Windows operating system nodes will reside. This storm protection will prevent broadcast or multicast storms caused by a node that is infected and using a denial-of-service attack. Normal FTE traffic of broadcast and multicast is well below 1% for each.

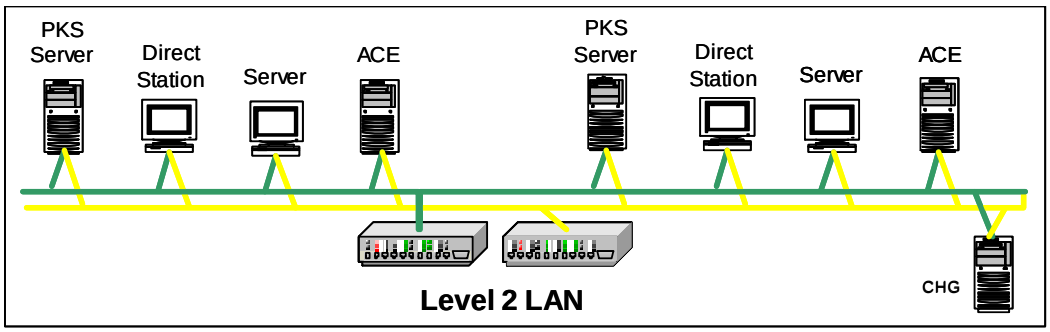
## 2.3 Level 2

### Description

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:**

- Cisco 2950 Switches
- PKS Server
- Server Stations
- Direct Stations
- ACE
- Subsystem Interfaces

**Level 2 Cisco 2950 Switches Provide:**

- Point-to-point connectivity for Level 2 devices
- High reliability configuration:
- 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

### Level 2 best practices

The switches in Level 2 are configured to provide the security and reliability as described in ”Connection of Level 1 nodes that intercommunicate using Level 2 switches” on page 30. 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 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.

An important best practice is to 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 instances 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.

### Complying with Level 2 best practices

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 need to have access to nodes on other subnets as well as access to certain nodes on Level 3 and possibly Level 4. Communication to other nodes may include Distributed Server Access (DSA), as well as engineering access to load control schemes and high-level control.
- 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 comply with Level 2 best practices

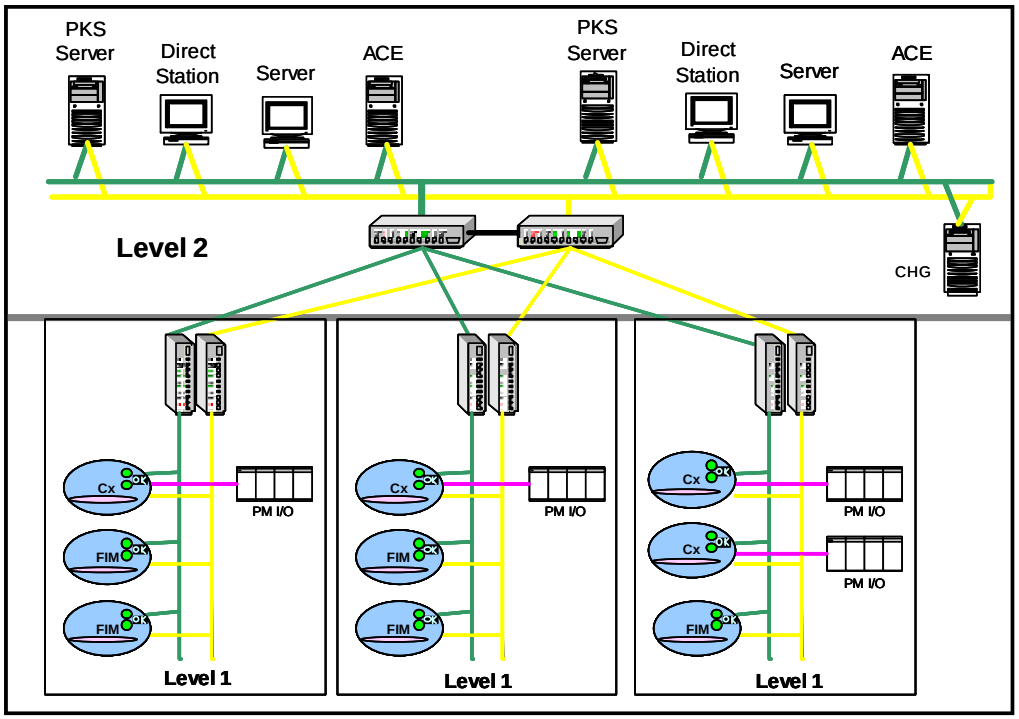
To accomplish this control, filtering is used in either the router, or the switch interface that connects to the router. Filtering, which is implemented by creating specific access lists for the Cisco equipment, must accomplish the following:

- Allow servers to have complete two-way communication with other nodes on the Level 2, Level 3 and Level 4 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.

Communication between Level 2 nodes and Level 3 Domain Controllers can be accomplished by adding access lists that enable *established* communications to return TCP packets from the Level 3 nodes to the initiating Level 2 nodes. Additionally, communications occur using UDP packets for Kerberos and LDAP. The filter must allow specific TCP port numbers used for these packets. See Section 6 for examples of access lists to be used for filtering.

### Level 2 to Level 1 connectivity

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 Switches:**

- Prioritize CDA traffic in high priority switch queue.
- Prioritize non-CDA traffic in low priority switch queue
- Ensure Level 2 to Level 1 supervisory traffic cannot disrupt Level 1 control traffic.

**Level 2 Switches:**

- Provide Level 1 to Level 2 connectivity
- Provide bandwidth limits for broadcast, multicast storm suppression.
- Preconfigure CDA traffic in High Priority Switch Queue (e.g., ACE-ACE, ACE-Cx, ACE-FIM, Server-Cx, Server-FIM).
- Preconfigure non CDA traffic in Low Priority Switch Queue.

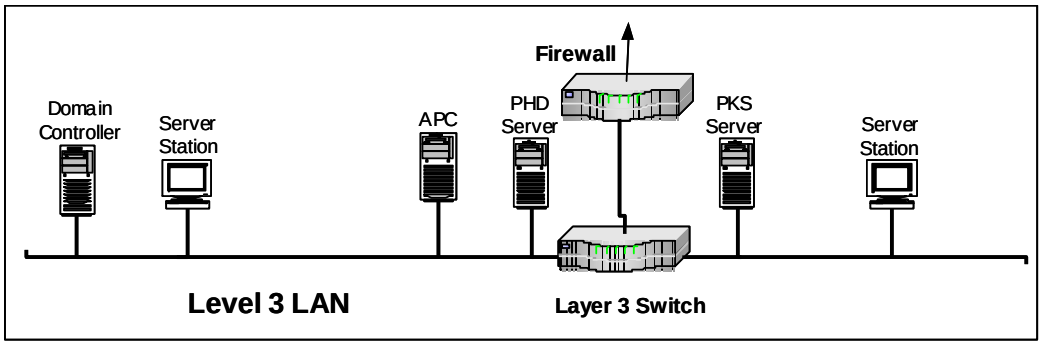
# 2.4 Level 3

## Description

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.

## 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 PKS Servers
- Server Stations (Monitoring)
- Engineering Stations

### 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.

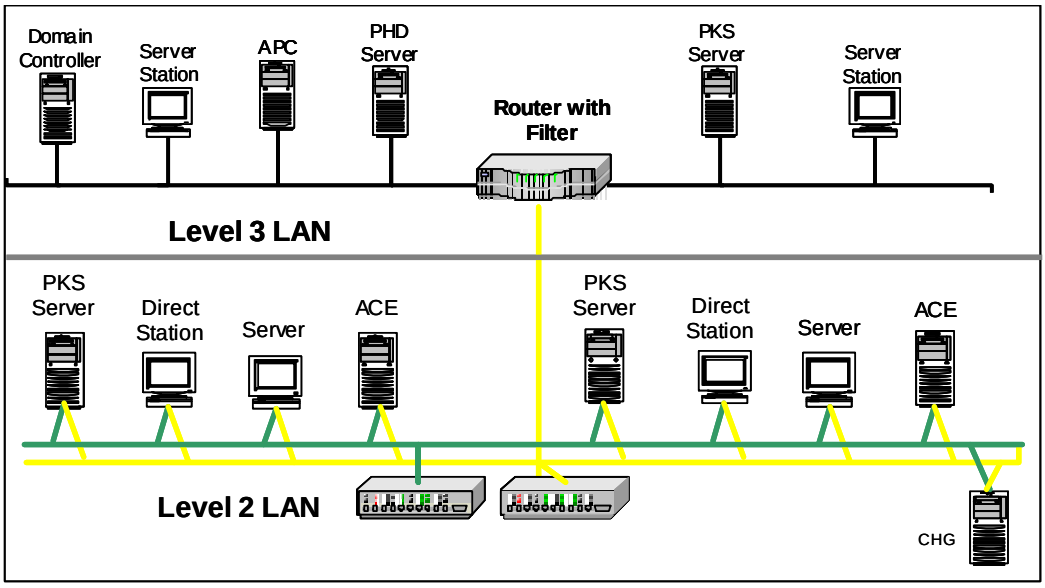
### Implementing Level 3 best practices

The following list summarizes the networking configuration requirements for Level 3 of the FTE network:

- Provide access between FTE subnets by grouping servers into an IP address range that can be separated from the other Level 2 nodes through use of a subnet mask, as discussed in Section 2.3.
- For Level 3 routers, enable IP multicast routing for the DSA multicast address, which is 225.7.4.103, and create an access-list filter to allow only this multicast address to pass to the FTE subnets.
- 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.
- 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 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 GBIC based interface.

### Level 3 to Level 2 connectivity

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

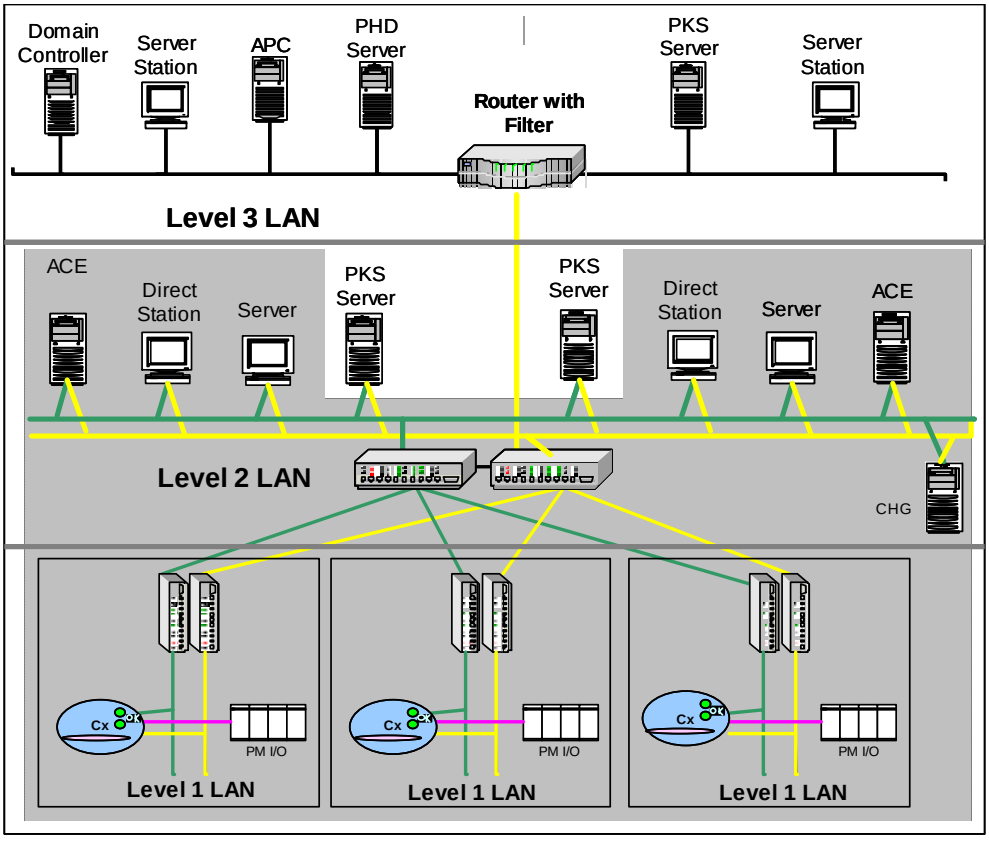



**Routers and filter:**

- Cisco 4xxx or 3550 series router recommended 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. Nodes not visible are shaded in gray. Notice that only the PKS 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 Switch (Cisco 3550/4xxx/6500 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 (L3 DC's and L2 Nodes requiring authentication

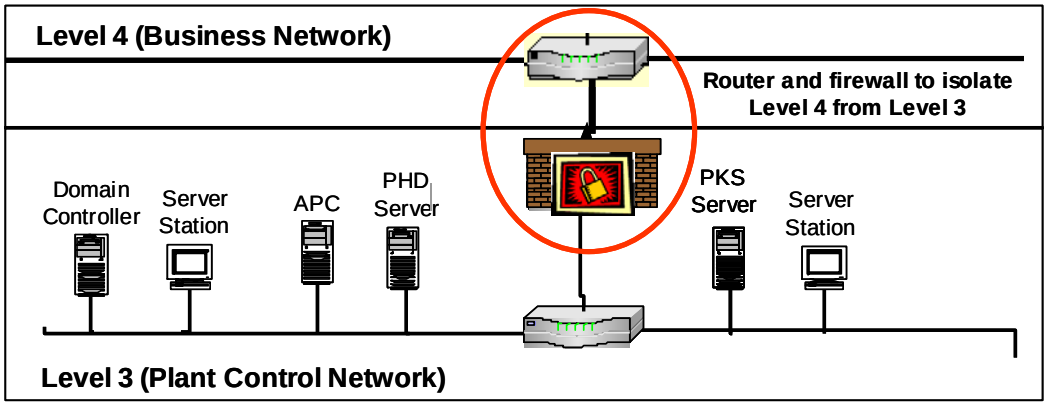
# 2.5 Level 4

## Description

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.




## Router

The router-to-firewall connection should be a single point of connectivity. This enables higher security and improved management. A major advantage of which 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

The firewall enables a restrictive security policy for traffic between Level 4 and Level 3. The firewall 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.

### 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.

### Implementing Level 4 best practices

The following list summarizes the 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 (NAT). See Section 3 for detailed information on IP address range selection, including the use of NAT.
- The firewall should limit the communication to only those nodes on Level 4 that require access to nodes on Level 3 or Level 2.
- 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.

### Using a router between Level 3 and Level 4

To enable higher security and improved management, the router-to-firewall connection should be a single point of connectivity. This allows the user to create an “air gap” between Level 3 and Level 4 by pulling a single cable. The connection to the firewall isolates Enterprise LAN Broadcast and Multicast traffic while enabling connectivity between the PCN and Enterprise LAN.

### Using a firewall between Level 3 and Level 4

The firewall enables a restrictive security policy for traffic between Level 4 and Level 3. The firewall should deny all access to the PCN unless it is explicitly permitted. A best practice is to use IP address source and destination filtering to permit only specific nodes on the enterprise network 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). Honeywell recommends TCP port filtering to stop denial-of-service attacks to well-known ports.

# 2.6 Configuration Rules for a Robust FTEB-based Topology

### Overview

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 supports three different standard Cisco 2950 Switch configuration options.

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 2.3. In this configuration Level 2 “mixed node” configuration script should be used. This configuration is typical for small cost-sensitive systems.

# 2.7 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 console station on Level 1 switches

In some instances, such as those previously described, it is acceptable to put the Level 2 console station directly on the Level 1 switches. However, 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 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.

For these mixed configurations, Honeywell recommends you use the switch configuration files with mixed interface programming. Future releases will have more filtering on the Level 1 switch that will preclude having Level 2 nodes attached. The best practice for security is to use separate Level 1 switches.

### 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 mixed switch configuration file would again 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.

# 3. Use of IP Addresses in an FTE Network

## 3.1 Introduction

### Importance of security

With the FTEB, Experion PKS R200 introduces controller nodes to the FTE community. With this addition of controllers, 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.

### FTE network 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* DSA communications
- FTE communities connected to Level 4 with DSA communications

### Overview of 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 | Even with complete isolation, 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<br>Simple address range configuration |
| FTE Communities connected to Level 4 with no DSA communications | Private IP addresses with a firewall that performs Network Address Translation (NAT) for communication with Level 4.<br>Dedicated Cisco equipment for the firewall.<br>Placement of servers in a separate range from other Level 2 nodes. |
| FTE communities connected to Level 4 with DSA communications | Unique Level 2 and Level 3 addresses that are compatible with Level 4 addresses.<br>Do not use NAT.<br>A method that conserves addresses, although it is more difficult to configure.<br>A subnet size that covers all Level 2 nodes.<br>A server range contained in the lower addresses that allows the other Level 2 nodes to start on a power of 2 boundary.<br>A reserved subnet size that can be used for the largest Level 1 range in the plant. |

## 3.2 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 DSA-connected communities. 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<br>Multiple FTE communities can be connected with a router. | First FTE subnet would be 10.**1**.X.Y<br>Second FTE subnet would be 10.**2**.X.Y |

### FTE Communities connected to Level 4 with *NO* DSA 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. In this case, a firewall that performs Network Address Translation (NAT) is necessary to convert private addresses to corporate network addresses. Honeywell recommends dedicated firewall equipment from Cisco be used, and does NOT recommend the use of a Windows-based PC with firewall software.

### 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" as described in the following table.

| Octet | Description | Example |
|---|---|---|
| CN | FTE community number | First FTE subnet would be 10.**1**.X.Y<br>Second FTE subnet would be 10.**2**.X.Y |
| X | Range of addresses where the two types of nodes exist.<br>Servers must be in a separate range from other Level 2 nodes. | 10.1.**0**.Y for server nodes<br>10.1.**1**.Y for station nodes<br>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 | 10.0.2.**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 10.0.4.Y range.<br>Level 3 nodes must not be able to communicate with Level 1 nodes. The nodes will have the following subnet masks:<br>• Level 2 Servers and console stations with communication to Level 1 nodes: 255.255.248.0.<br>• Level 2 nodes with no communication to Level 1 nodes: 255.255.252.0.<br>• Level 1 controller nodes: 255.255.248.0.<br>• Level 3 router interface to Level 2: 255.255.252.0. |

### FTE communities connected to Level 4 with DSA communications

Some installations require DSA or DCOM based communication between Level 4 nodes and Level 2 nodes. In this case, the Level 2/Level 3 addresses must be unique and compatible with Level 4 addresses, and NAT cannot be used.

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 for IP address distribution: FTE communities connected to Level 4 with DSA

Table 3-1 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 128 nodes. The address distribution would be:

**Table 3-1 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 64 nodes. |
| 164.1.0.2-15 | Server nodes (5 servers 2 addresses each starting at address 2 rounded up to power of 2).<br>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.<br>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).<br>The subnet mask is 255.255.255.128 to cover the Level 1 and Level 2 range. |
| 164.1.0.64-128 | All access from Level 3 is blocked by the subnet mask of 255.255.255.192 on the interface to the FTE community. |

## 3.3 Reusing IP Addresses for Level 1

### Purpose

Level 1 devices have the potential to consume many thousands of IP addresses in a corporate IP address space. To conserve corporate IP addresses, Honeywell recommends an address reuse scheme.

### 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.

# 3.4 Allowing Level 1 to Level 2 Communication

### Purpose

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.

### Configuring a route add command

For 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. Nodes that do not communicate with the Level 1 nodes do not need the "route add" configured. The following example shows the command for a Level 2 node in which the:

- 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.

### Level 2 address ranges

In addition to the route add command, for Level 1 nodes to communicate with Level 2 nodes, the Level 2 address range must be a subset of the Level 1 range so that a subnet mask will allow communication between Level 1 and Level 2. Using the previous example:

- If the Level 2 address range is 164.1.0.0 to 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 via 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.

# 4. Switch Installation and Configuration

## 4.1 Introduction

### Overview

The specific tasks you need to perform depend on the switch model number you are installing. This section contains procedures for the following tasks:

- Using Switch Configuration Files
- Installing and Configuring a Cisco Switch
- Saving and Modifying Cisco Switch Configuration Files
- Installing and Configuring a Nortel Switch
- Preventing Crosslink Errors

### Assumptions

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 latest Software Change Notice (SCN), which provides last-minute changes, special instructions, and workarounds |

## 4.2 Using Switches in an FTE Network

### 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 disabled should remain for existing Nortel switches in an FTE community.

### 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<br><br>Must have the speed set to 100 Megabit and full duplex | Cisco does not recommend using this feature when connecting to other switches.<br><br>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. Procedures for using these configuration files are included in Section 4.3 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.

### FTE switch 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 using either a crossover cable or a router. |
| 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. |

# 4.3 Using Switch Configuration Files

### About Cisco switch configuration requirements

Honeywell provides a set of switch configuration files on the Common Component CD that, when implemented, configure the FTE switch ports for different node types according to defined requirements. See Table 4-2 for a complete list of all files. 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 |

### 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:

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

### Cisco switch and port options

After installing the redundant pair of switches, you will need to configure the Cisco switches for FTE 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, are used to configure the various switch and port options as listed in Table 4-1. Additionally, the configuration files contain Quality of Service parameters that are attached to the ports.

**Table 4-1 Cisco Switch and Port Options**

| Option Types | Available Options |
|---|---|
| **Switch options** | 2950-24 |
| | 2950-48 |
| | 2955C-12 |
| | 3550-12 |
| | 3550-24FX |
| **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. |

### 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.

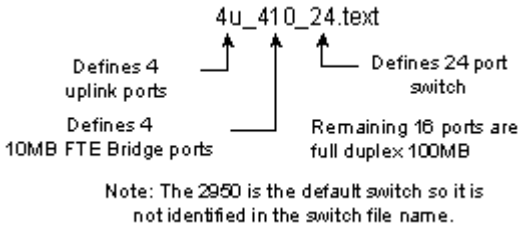
**Figure 4-1 Cisco Switch Port Configuration**

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

### Switch configuration examples

Following are examples of how switch ports are configured using the switch configuration files.

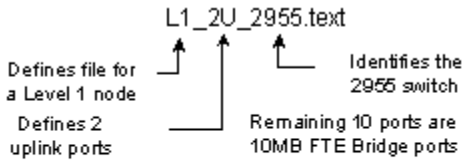
#### *Cisco 2950-24 switch: 4 uplink ports, 4 FTE Bridge ports, 16 FD 100MB ports*




Note: The 2950 is the default switch so it is not identified in the switch file name.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **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** |

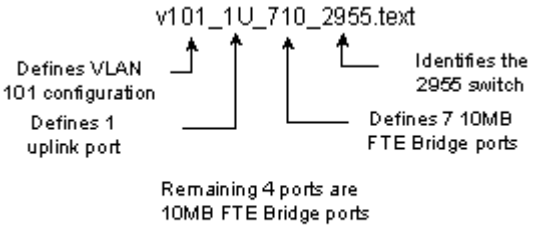
#### *Cisco 2955-12 switch: Level 1, 2 uplink ports, 10 10MB FTE Bridge ports*




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** |

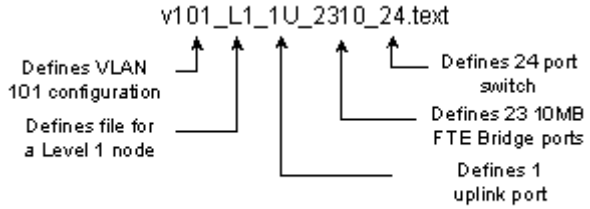
***Cisco 2955-12 switch: V101 configured, 1 uplink port, 7 10 MB FTE Bridge ports, 4 FD 100 MB ports***




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***




Note: The 2950 is the default switch so it is not identified in the switch file name.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **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** |

### Switch configuration files

Table 4-2 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 4-2 FTE Switch Configuration Files**

| Switch configuration file | 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_2u_2210_24 | 1 | 2950-24 | 2 | 22 | 0 | No |
| v101_L1_1u_2310_24 | 1 | 2950-24 | 1 | 23 | 0 | Yes |
| v101_L1_2u_2210_24 | 1 | 2950-24 | 2 | 22 | 0 | Yes |
| L1_1u_4710 | 1 | 2950-48 | 1 | 47 | 0 | No |
| v101_L1_1u_4710 | 1 | 2950-48 | 1 | 47 | 0 | Yes |
| L1_1u_2955 | 1 | 2955C-12 | 1 | 11 | 0 | No |
| L1_2u_2955 | 1 | 2955C-12 | 2 | 10 | 0 | No |
| v101_L1_1u_2955 | 1 | 2955C-12 | 1 | 11 | 0 | Yes |
| v101_L1_2u_2955 | 1 | 2955C-12 | 2 | 10 | 0 | Yes |
| 12u_24 | 2 | 2950-24 | 12 | 0 | 12 | No |
| 2u_24 | 2 | 2950-24 | 2 | 0 | 22 | No |
| 4u_24 | 2 | 2950-24 | 4 | 0 | 20 | No |
| v101_12u_24 | 2 | 2950-24 | 12 | 0 | 12 | Yes |
| v101_2u_24 | 2 | 2950-24 | 2 | 0 | 22 | Yes |
| v101_4u_24 | 2 | 2950-24 | 4 | 0 | 20 | Yes |
| 2u | 2 | 2950-48 | 2 | 0 | 46 | No |
| 4u | 2 | 2950-48 | 4 | 0 | 44 | No |
| v101_2u | 2 | 2950-48 | 2 | 0 | 46 | Yes |
| v101_4u | 2 | 2950-48 | 4 | 0 | 44 | Yes |
| fte_3550_cnfg | 2 | 3550-12 | 12 | 0 | 0 | No |
| v101_fte_3550_cnfg | 2 | 3550-12 | 12 | 0 | 0 | Yes |
| 24u_3550fx | 2 | 3550-24FX | 24 | 0 | 0 | No |
| v101_24u_3550fx | 2 | 3550-24FX | 24 | 0 | 0 | Yes |

**Table 4-2 FTE Switch Configuration Files**

| Switch configuration file | Level | Switch Type | No. of uplinks | No. of 10 MB FTEBs | No. of FD 100 MBs | VLAN101 configured |
|---|---|---|---|---|---|---|
| 4u_1610_24 | 1 & 2 | 2950-24 | 4 | 16 | 4 | No |
| 4u_410_24 | 1 & 2 | 2950-24 | 4 | 4 | 16 | No |
| 4u_810_24 | 1 & 2 | 2950-24 | 4 | 8 | 12 | No |
| v101_4u_1610_24 | 1 & 2 | 2950-24 | 4 | 16 | 4 | Yes |
| v101_4u_410_24 | 1 & 2 | 2950-24 | 4 | 4 | 20 | Yes |
| v101_4u_810_24 | 1 & 2 | 2950-24 | 4 | 8 | 12 | Yes |
| 4u_1610 | 1 & 2 | 2950-48 | 4 | 16 | 28 | No |
| 4u_410 | 1 & 2 | 2950-48 | 4 | 4 | 40 | No |
| 4u_810 | 1 & 2 | 2950-48 | 4 | 8 | 36 | No |
| v101_4u_1610 | 1 & 2 | 2950-48 | 4 | 16 | 28 | Yes |
| v101_4u_410 | 1 & 2 | 2950-48 | 4 | 4 | 40 | Yes |
| v101_4u_810 | 1 & 2 | 2950-48 | 4 | 8 | 36 | Yes |
| 1u_710_2955 | 1 & 2 | 2955C-12 | 1 | 7 | 4 | No |
| v101_1u_710_2955 | 1 & 2 | 2955C-12 | 1 | 7 | 4 | Yes |

# 4.4 Installing and Configuring a Cisco Switch

### Overview

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.

### Passwords and names for switch access and configuration

During the switch configuration process, you will be 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* |

### 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. |

### Tasks for configuring a Cisco Switch

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

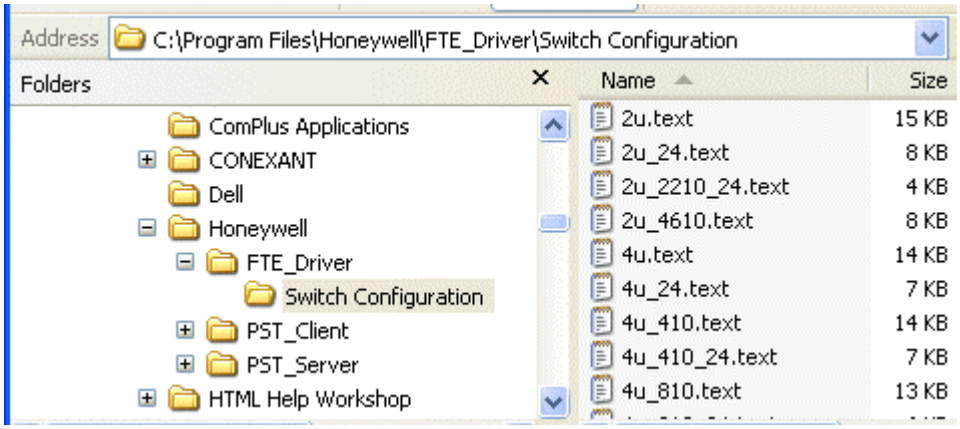
**Table 4-3 Cisco Switch Configuration Tasks**

| ✓ | Task |
|---|---|
| | Connect to the switch |
| | Configure switch interface options |
| | Load the appropriate switch configuration file |

### Accessing switch configuration files

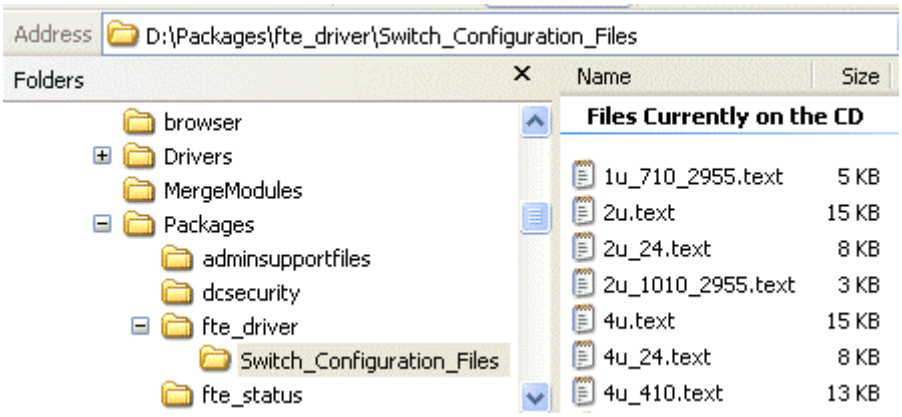
Switch configuration files are packaged with the FTE Driver and will be copied to the following location when you run the FTE Driver installation package.

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




If you have not yet installed FTE, you may access switch configuration files from the Honeywell Common Components CD 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 4-4 Conventions Used to Convey Instructions and Information**

| | |
|---|---|
| `At any point you may enter a question mark '?' for help.`<br>`Use ctrl-c to abort configuration dialog at any prompt.`<br>`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`**<br>`Enter configuration commands, one per line. End with CNTL/Z.`<br>`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>`<br>`Writing config.text !!!!` | Nonprinting characters, such as passwords or Enter key, are in angle brackets (< >). |

### Connect 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:<br>• Bits per second: 9600<br>• Data Bits: 8<br>• Parity: NONE<br>• Stop bits: 1<br>• Flow control: Xon/Xoff |
| **8** | Click **OK.** |
| **9** | Power up the switch and go to the next procedure. |

### Configure 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 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**<br>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.<br><br>Press the space bar to advance the display when it pauses. |

| Step | Action |
|---|---|

```
Current interface summary


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

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

FastEthernet0/48       unassigned      YES  unset   down           down
GigabitEthernet0       unassigned      YES  unset   down           down
GigabitEthernet0/2     unassigned      YES  unset   down           down
```

**5** After the configuration display is complete, the switch dialog appears.

Type all values that appear in **bold**.

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

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

**6** The following is an abridged example of what displays after the **vlan1** configuration.

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

| Step | Action |
|---|---|

```
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.<br>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:<br>• To configure vlan1, type **int vlan1**, or<br>• To configure vlan101, type **int vlan101**:<br>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:<br>***10.1.4.253 255.255.255.0***<br>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:<br>***ps_user*** **-** example user name<br>***ps_user local*** **–** example password<br>***FTE4*** **–** example virtual terminal password<br>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. Each switch should also have a community name.<br><br>The following are used as the examples in the switch displays:<br><br>***10.1.4.15*** - EPKS Server IP address<br><br>***FTE*** **-** Switch Community Name<br><br>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<br>**#snmp-server host *10.1.4.16 FTE* snmp**<br>command using the redundant server IP address (***10.1.4.16*** – is used as an example for the redundant server IP address). |

**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 |
|---|---|
| **16** | The following are used as examples in the switch displays:<br><br>***10.1.4.1***- Default gateway IP address<br><br>***192.168.100.1*** - NTP Time Server IP address<br><br>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
```

| | |
|---|---|
| **17** | Configure the NTP timeserver.<br><br>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
```

| | |
|---|---|
| **18** | Type **exit**.<br><br>Type **write**.<br><br>The switch configuration is complete. |

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

| | |
|---|---|
| **19** | 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 4-2 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 desired VLAN number.

### Load the appropriate switch configuration file

The following procedure uses Hyperterm's Xmodem file transfer utility to transfer the correct switch configuration file from the installation CD to the switch. See Table 4-2 in for details on each switch configuration file. After downloading the switch configuration file to the switch, 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 4-2 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>
```

| | |
|---|---|
| **3** | Initiate the transfer in Hyperterm and choose the appropriate switch configuration file:<br>• From the Hyperterm menu bar, select **Transfer > Send File**.<br>• Select Browse and navigate to the **Switch Configuration** folder in the following location:<br>– *C:\Program Files\Honeywell\FTE_Driver\, or*<br>– *Media Drive:\Packages\FTE_Driver\Switch_Configuration_Files*<br>• Select the correct switch configuration file for your particular system and click **OPEN**.<br>• Select **Xmodem** under **Protocol**.<br>• 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
```

| Step | Action |
|---|---|
| **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:<br>• 4 uplink ports<br>• 4 autospeed ports for FTEB<br>• Remaining ports at 100 MB<br>Press the space bar to advance the display when it pauses. |

```
Building configuration...

Current configuration : 15560 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service sequence-numbers
!
hostname Cisco_FTE4
!
enable secret 5 $1$JIQ6$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
```

| Step | Action |
|---|---|

```
class-map match-all cda_low
  match access-group 105
!
!
policy-map cda_policy
  class cda_urgent
    set ip dscp 56
  class cda_high
    set ip dscp 46
!
ip subnet-zero
ip ftp username ps_user
ip ftp password ps_user local
no ip igmp snooping
!
spanning-tree extend system-id
!
!
interface FastEthernet0/1
 no ip address
 duplex full
 speed 100
 service-policy input cda_policy
 storm-control broadcast level 20.00 18.00
 storm-control multicast level 20.00 18.00
 storm-control unicast level 20.00 18.00
 storm-control action trap

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

 storm-control multicast level 20.00 18.00
 storm-control unicast level 20.00 18.00
```

| Step | Action |
|---|---|

```
 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
```

| Step | Action |
|---|---|

```
access-list 105 permit udp any any eq 55560
access-list 105 permit tcp any any eq 55559
access-list 105 permit udp any any eq 12321
access-list 105 permit tcp any any eq 55556
access-list 105 permit tcp any any eq 55557
access-list 105 permit tcp any any eq 55558

!
line con 0
 exec-timeout 0 0
line vty 0 4
 password FTE1
 login
line vty 5 15
 password FTE1
 login
!
end

Cisco_FTE4#
```

**10** This is the end of the switch configuration. If you would like to archive the configuration file for future use, see Section 4.5.

# 4.5 Saving and Modifying Cisco Switch Configuration Files

### Overview

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.

### Download 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.<br><br>***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.<br><br>Type the virtual terminal password you previously configured for the switch and press Enter.<br><br>***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:<br><br>***Cisco_FTE1*** is used in the following example.<br><br>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.<br><br>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.<br><br>***10.1.4.15*** is used in the following example.<br><br>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.

# 4.6 Installing and Configuring a Nortel Switch

### Overview

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 that will 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 4-5 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 Ethernet switch |
| | Configure the connection speed for switch ports |
| | Connect crossover cables |

### Disable Snooping and Spanning Tree on Ethernet 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 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:<br>• Bits per second: 9600<br>• Data Bits: 8<br>• Parity: NONE<br>• Stop bits: 1<br>• Flow control: Xon/Xoff |

| Step | Action |
|---|---|
| **8** | Verify the connection between the computer and the switch. |
|  | **TIP**<br>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**<br>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. |

# 5. Network Troubleshooting

## 5.1 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 5-1 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.<br>Cable with the green boot is connected to the Switch in the *Green* Tree, but it is connected to first port.<br>Connection for first port (cable with yellow boot) is connected to the Switch in the *Green* Tree.<br>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.<br>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:<br>• FTE Network has more than one crossover cable<br>• Multiple connections to an external network<br>• Switches are not in a tree hierarchy |

# 6. Switch and Router Configuration Examples

## 6.1 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
```

## 6.2 Cisco Router Configuration Statements Examples

### Purpose

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.

# 6.3 Subnet Mask Derivation

### Overview

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).

### Examples

#### *L2-L3 Router Port Netmask:*

- 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:*

- 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*

- 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