CHAPTER 6

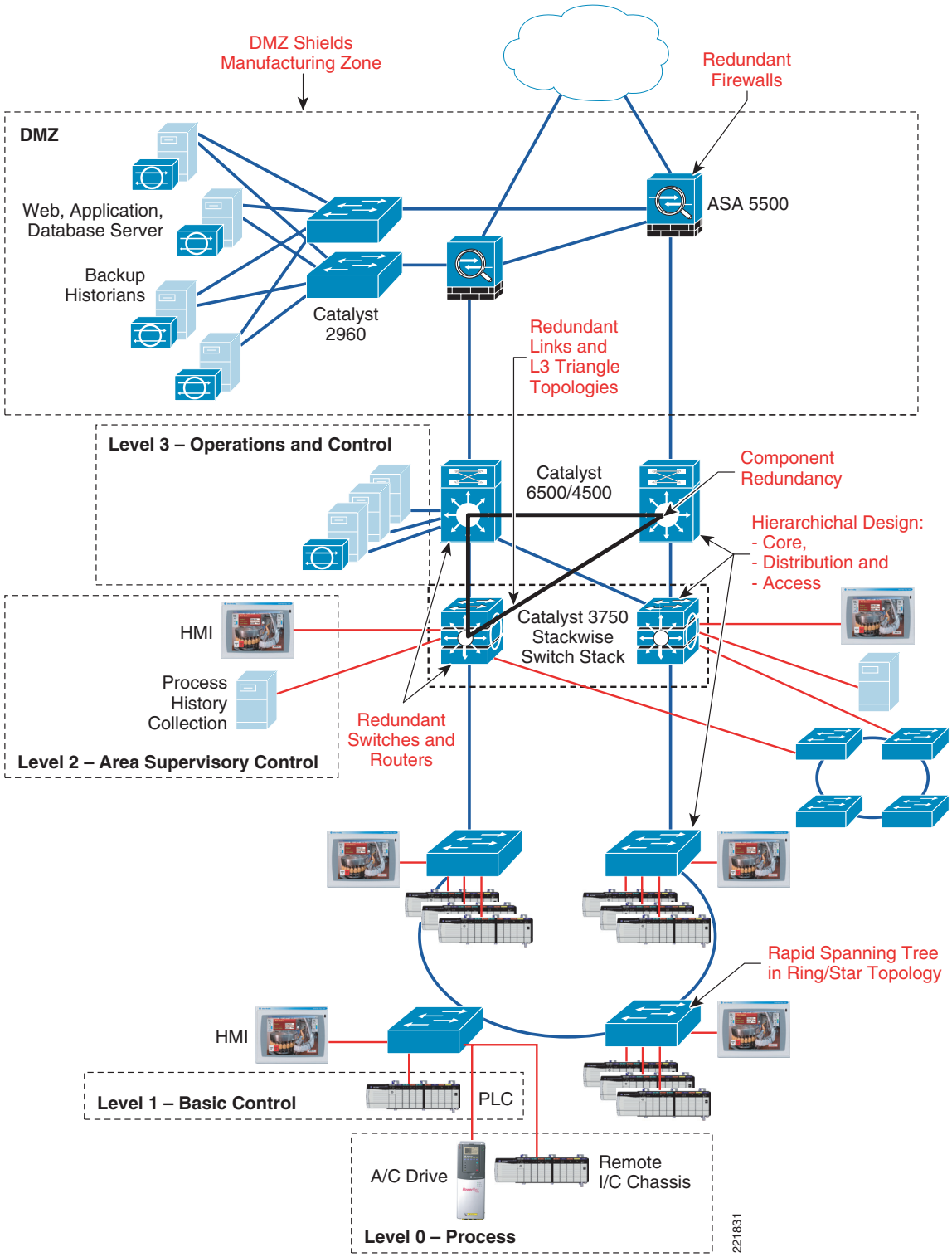
Implementation of High Availability

High availability (HA) is not a standalone feature, but instead an approach to implementing a variety of interrelated features as tools to ensure business resilience and maintain end-to-end availability for services, users, devices, and applications. High availability should be incorporated at many layers. With a sound design, network stability is easy to achieve, troubleshooting is easier, and human error is reduced. Key aspects of an HA network include the following:

- Hierarchical network design based on both the EttF logical architecture and the enterprise campus core-distribution-access model
- Network and component redundancy that includes both redundant network systems, links, and systems with redundant components
- Foundation services that apply the network software features to maintain network availability when links, components, or other failures occur

Figure 6-1 shows the key high availability features that Cisco recommends for the EttF solution architecture.

Figure 6-1 Recommended High Availability Features



Cisco HA is technology delivered in Cisco IOS Software that enables network-wide resilience to increase network availability. Network applications must cross different network layers from the access, distribution, core, and DMZ. High availability in a manufacturing environment consists of both network resiliency and system resiliency, which when combined result in transparent fault detection and recovery to the user community. An unscheduled network failure that is not resolved can result in termination, interruption, or violation of service-level agreements (SLAs) for manufacturing business-critical applications.

This chapter includes the following topics:

- Overall benefits of an HA design
- Best practices and HA modeling
- Design considerations and best practices for HA in the cell/area zone
- Design considerations and best practices for HA in the manufacturing zone
- Design considerations and best practices for HA in the DMZ

For an overview of general HA topics, see *Designing a Campus Network for High Availability* at the following URL: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/cdccont_0900aecd801a8a2d.pdf.

Benefits of an HA Design

Unscheduled downtime has many costs. On a manufacturing shop floor, downtime can result in revenue losses that directly affect the bottom line. Table 6-1 shows availability percentages and downtime per year.

Table 6-1 Availability and Downtime

Availability	Defects Per Million	Downtime Per Year
99.9000%	1000	8 hours, 46 minutes
99.9500%	500	4 hours, 23 minutes
99.9900%	100	53 minutes
99.9990%	10	5 minutes
99.9999%	1	30 seconds

A highly available network design improves SLA support, reduces unplanned downtime, and increases operational efficiencies. High availability is a function of the application as well as the end-to-end network connectivity between a factory floor node and a specific service. These services can be device communication within the cell/area zone, or application traffic to or from the manufacturing zone and DMZ. With an effective HA design, a more deterministic network is available, which influences overall network availability. Key considerations are the mean time between failures (MTBF) and mean time to repair (MTTR).

Best Practices and HA Modeling

For the network to be deterministic, the design must be as simple and highly structured as possible. This is achieved by implementing a network hierarchy. Recovery mechanisms must be considered as part of the design process. Recovery timing is determined in part by the nature of the failure; for example, total device failure, direct link failure, indirect link failure, and so on. Several key components and design concepts are examined in the following sections at each network layer.

Before implementing an HA solution, it is wise to use a modeling exercise, for both the network infrastructure and the network connections, to validate the architecture/design, justify costs, and analyze design tradeoffs.

Device modeling concerns include each field-replaceable unit as well as critical components such as supervisors, power supplies, and line cards. Device modeling includes the following steps:

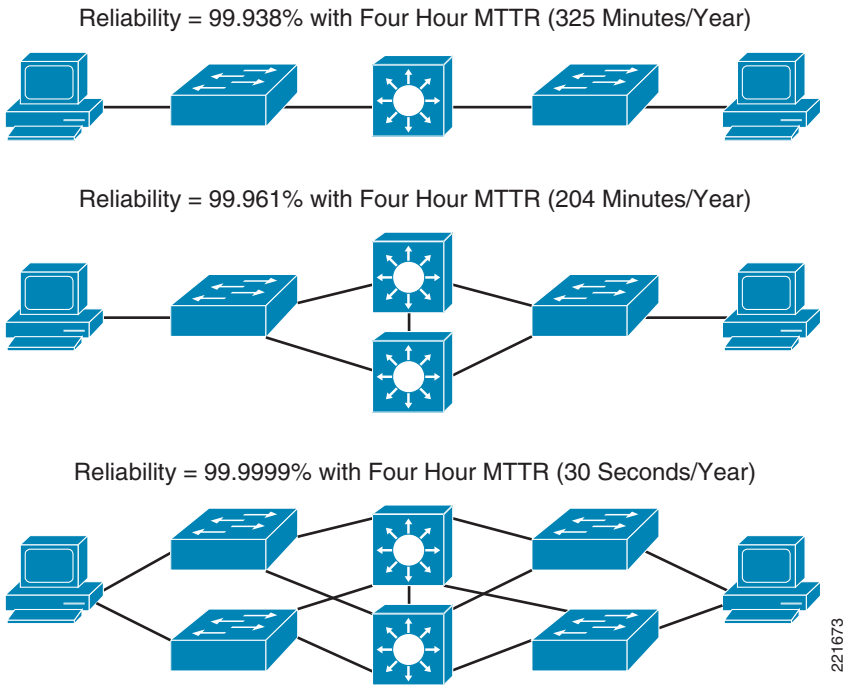
1. Describing the system and traffic path
2. Building a system block diagram
3. Describing failure scenarios
4. Running the model

Network modeling is concerned with network resiliency, which involves redundant links and alternate paths. Network modeling includes the following steps:

1. Describing the system and traffic path
2. Building a system block diagram
3. Describing failure scenarios
4. Running the device model from above
5. Running the network model

See Figure 6-2 for an example of network reliability models with an MTTR of four hours.

Figure 6-2 Network Reliability Models



HA Design in the Cell/Area Zone

The cell/area zone devices, Cisco Catalyst 2955 Series switches, rely mainly on a redundant network design (star or ring) to achieve high availability. These are the Layer 2-only access devices in the Cisco core-distribution-access model, and care must be taken to achieve some resiliency at this level because this is the first network connection point from the end-node perspective. (See Table 6-2.)

Table 6-2 Summary of Features in the Cell/Area Zone

Feature	Description
Redundant power supplies	Each Cisco Catalyst 2955 can have an external power supply installed.
Redundant paths	Depends on topology (either star or ring).
StackWise	Uses stack interconnect cables to create a virtual switch fabric for stacks of the Catalyst 3750.
Broadcast storm control	Storm control uses rising and falling thresholds to block and then restore the forwarding of broadcast, unicast, or multicast packets. You can also set the switch to shut down the port when the rising threshold is reached. This is good for STP misconfiguration or a bad cable.
Rapid Spanning Tree Protocol	Layer 2 protocol to prevent loops in the network. This mode of spanning tree is preferred for the best convergence times if a failure occurs.

HA Design and Implementation in the Manufacturing Zone

Depending on the topology choice, either two access layer switches (ring) or all access layer switches (star), have uplinks terminating on a pair of redundant Layer 3 switches, which act as an aggregation point. This aggregation layer is referred to as the distribution layer. The distribution layer is the first place where routing and Layer 3 switching occur in the multilayer model. Important features provided by this layer include the following:

- Default gateway redundancy
- Intelligent best-path selection towards other modules of the network
- Wire-speed Layer 3 switching

For EttF 1.1, two stacked Cisco Catalyst 3750s are chosen to fulfil this role (see Figure D-1). With StackWise technology, switch redundancy is achieved, but logically only one switch is being managed and configured.

The uplinks on the Catalyst 3750s from the distribution layer to the core layer are cross-stack Layer 3 EtherChannels, which provide yet another level of redundancy and resiliency in the event of a link failure (see Figure D-1). EtherChannels also provide additional bandwidth by aggregating up to eight interfaces into one logical interface. The core layer, with dual Cisco Catalyst 4507R switches, achieve the maximum device redundancy with redundant supervisors and power supplies. From a link and alternate path perspective, meshed connections down to the Cisco Catalyst 3750 are recommended.

Following is a sample Catalyst 3750 cross-stack EtherChannel configuration:

```
!
interface GigabitEthernet1/0/25
 no switchport
 no ip address
 channel-group 1 mode active
end

CZ-C3750-1#show run int g2/0/25
Building configuration...

Current configuration : 98 bytes
!
interface GigabitEthernet2/0/25
 no switchport
 no ip address
 channel-group 1 mode active
end

CZ-C3750-1#show run int p1
Building configuration...

Current configuration : 108 bytes
!
interface Port-channel1
 description CZ-C4500-1
 no switchport
 ip address 10.18.3.100 255.255.255.0
end

CZ-C3750-1#show ether summ
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
```

```
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 4
Number of aggregators:           4

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(RU)         LACP      Gi1/0/25(P) Gi2/0/25(P)
2      Po2(SD)          -
3      Po3(RU)         LACP      Gi1/0/27(P) Gi2/0/27(P)
10     Po10(SD)        LACP      Gi1/0/1(D)  Gi2/0/1(D)

Sample 4500 EtherChannel Configuration

interface GigabitEthernet4/9
 no switchport
 no ip address
 logging event link-status
 channel-group 1 mode active
end

CZ-C4500-1#show run int g4/10
Building configuration...

Current configuration : 123 bytes
!
interface GigabitEthernet4/10
 no switchport
 no ip address
 logging event link-status
 channel-group 1 mode active
end

CZ-C4500-1#show run int p1
Building configuration...

Current configuration : 96 bytes
!
interface Port-channel1
 ip address 10.18.3.101 255.255.255.0
 logging event link-status
end

CZ-C4500-1#show ether summ
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 4
Number of aggregators:           4

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(RU)         LACP      Gi4/9(P)    Gi4/10(P)
```

First Hop Redundancy

For EttF 1.1, first hop redundancy is the default gateway that end nodes have configured in case they need to communicate across subnets. For cell/area-level devices (PACs, VFDs, I/O), the default gateway is configured on the SVI terminating the VLAN(s) carried in the cell/area zone. Two Catalyst 3750s are stacked together to form one logical router, so in the case of a single router failure, the second stacked Catalyst 3750 takes over as the default gateway. Note, however, that the default behavior is for the newly active stack master to assign a new stack MAC address. This can be a problem for end nodes that do not support Gratuitous Address Resolution Protocol (GARP), which sends a message to hosts to clear their ARP cache and to assign a new IP/MAC binding. As such, the **stack-mac persistent timer 0** command should be used to ensure that the original master MAC address remains the stack MAC address after a failure. This makes it transparent to endpoints, so that they do not have to learn a new IP/MAC pair. The following is a sample session:

```
CZ-C3750-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CZ-C3750-1(config)#
CZ-C3750-1(config)#stack-mac persistent timer ?
  <0-0>   Enter 0 to continue using current stack-mac after master switchover
  <1-60>  Interval in minutes before using the new master's mac-address
  <cr>

CZ-C3750-1(config)#stack-mac persistent timer 0
```

For application servers, which are connected to a separate Layer 2 switch that is connected to the dual Catalyst 4507R switches in the manufacturing zone (see Figure D-1), Cisco recommends using Hot Standby Routing Protocol (HSRP) as the method of providing first hop redundancy. A router is elected as the active router and is responsible for answering ARP requests for the virtual IP address. HSRP routers discover each other via hello packets, which are multicast packets sent to the 224.0.0.2 “all-routers” address (knowledge of this address may be important for troubleshooting purposes). Remember that HSRP is completely independent of the routing protocol in use on the router. For more information about HSRP, see the following URL:
http://www.cisco.com/en/US/docs/internetworking/case/studies/cs009.html

NSF/SSO

From a Layer 3 perspective, the default behavior of a router after a failover event is to tear down routing protocol neighbor relationships, re-establish the neighbor, relearn routing information, and re-populate the Cisco Express Forward table. This can take minutes, depending on the size of the routing table. In a manufacturing environment, this is unacceptable, so Nonstop Forwarding with Stateful Switchover (NSF/SSO) is recommended to mitigate that risk. For EttF 1.1, this applies only to the Catalyst 4507s and the Catalyst 3750s.

NSF works in conjunction with SSO to ensure Layer 3 integrity following a switchover. This allows a router experiencing the failure of an active supervisor to continue forwarding data packets along known routes while the routing protocol information is recovered and validated. This forwarding can continue to occur even though peering arrangements with neighbor routers have been lost on the restarting router. NSF relies on the separation of the control plane and the data plane during supervisor switchover. The data plane continues to forward packets based on pre-switchover Cisco Express Forwarding information. The control plane implements graceful restart routing protocol extensions to signal a supervisor restart to NSF-aware neighbor routers, reform its neighbor adjacencies, and rebuild its routing protocol database following a switchover. An NSF-capable router implements the NSF functionality and continues to forward data packets after a supervisor failure. An NSF-aware router understands the NSF

graceful restart mechanisms: it does not tear down its neighbor relationships with the NSF-capable restarting router, and can help a neighboring NSF-capable router restart, thus avoiding unnecessary route flaps and network instability. An NSF-capable router is also NSF-aware.

To configure SSO on the Catalyst 4507s, perform the following configuration:

```
CZ-C4500-1#conf t
CZ-C4500-1(config)#redund
CZ-C4500-1(config-red)#mode ?
  rpr  Route Processor Redundancy
  sso  Stateful Switchover

CZ-C4500-1(config-red)#mode sso
CZ-C4500-1(config-red)#
```

To configure NSF on the Catalyst 4507s, add the **nsf** keyword when configuring a dynamic routing protocol (note that OSPF is the selected IGP):

```
router ospf 100
 router-id 1.1.1.1
 log-adjacency-changes
 nsf
```

Summary of Features in the Manufacturing Zone

Table 6-3 provides a summary of features in the manufacturing zone.

Table 6-3 Summary of Features in the Manufacturing Zone

Feature	Description	Where To Apply in I.E Network
Redundant paths	Meshed connections for multiple paths.	• Catalyst 4500 • Catalyst 3750
Redundant route processors (supervisors)	Active and standby supervisors operate in active and standby modes, and provide a variety of redundancy mechanisms to handle failure scenarios.	• Catalyst 4500 • Catalyst 3750—Virtual with StackWise
StackWise	Uses stack interconnect cables to create a virtual switch fabric for stacks of the Catalyst 3750.	• Catalyst 3750 • N/A to other platforms
Redundant power supplies	Each system has dual power supplies so that the system operates normally upon failure of a power supply.	• Catalyst 4507R—Internal • Catalyst 3750—External • Catalyst 2955—External
Redundant fans	Each fan tray has multiple fans.	Catalyst 4507R
Line card online insert and removal (OIR)	New line cards can be added or removed without affecting the system or losing the configuration.	Catalyst 4507R
Nonstop Forwarding with Stateful Switchover (NSF with SSO)	Inter-chassis supervisor failover at Layers 2 through 4. Reduces the mean time to recovery (MTTR).	Catalyst 4507R

Table 6-3 Summary of Features in the Manufacturing Zone (continued)

Nonstop Forwarding Awareness	Processes NSF messages from restarting neighbor and does not tear down neighbor relationship.	Catalyst 3750
In-Service Software Upgrade (ISSU)	Ranges from full image upgrades to granular, selective software maintenance are able to be performed without service impact across all Cisco IOS-based products.	Catalyst 4507R
Automatic software upgrade for Catalyst 3750 StackWise	The master 3750 transfers the same version of code to the remaining switches in the stack. The upgrade includes: • Transferring the global configuration • Applying default configuration • Applying preconfigured configuration	Catalyst 3750
Generic Online Diagnostics (GOLD)	Online diagnostics to help ensure that a system booting up and a live system are healthy.	• Catalyst 4507R and 3750—Subset of GOLD
EtherChannel	Link aggregation for bandwidth and redundancy; both PAgP and LACP are supported.	Catalyst 4507R and 3750

HA Design and Implementation in the DMZ

Cisco ASA Redundancy Design

Cisco ASA supports the following two types of failover:

- Active/standby
- Active/active

Active/standby is the supported design for EttF 1.1, in which the active ASA is responsible for passing traffic. Active/standby failover allows a standby security appliance to take over the functionality of a failed unit. When the active unit fails, it changes to the standby state and the standby unit changes to the active state. The unit that becomes active assumes the IP addresses (or, for transparent firewall, the management IP address) and MAC addresses of the failed unit and begins passing traffic. The unit that is now in standby state takes over the standby IP addresses and MAC addresses. Because network devices see no change in the MAC-to-IP address pairing, no ARP entries change or time out anywhere on the network.

Primary/Secondary Status and Active/Standby Status

The main differences between the two units in a failover pair are related to which unit is active and which unit is standby; that is, which IP addresses to use and which unit actively passes traffic. However, the following differences exist between the units based on which unit is primary (as specified in the configuration) and which unit is secondary:

- The primary unit always becomes the active unit if both units startup at the same time (and are of equal operational health).
- The primary unit MAC addresses are always coupled with the active IP addresses. The exception to this rule occurs when the secondary unit is active, and cannot obtain the primary unit MAC addresses over the failover link. In this case, the secondary unit MAC addresses are used.

Determination of the Active Unit

The active unit is determined by the following:

- If a unit boots and detects a peer already running as active, it becomes the standby unit.
- If a unit boots and does not detect a peer, it becomes the active unit.
- If both units boot simultaneously, the primary unit becomes the active unit and the secondary unit becomes the standby unit.

Failover Triggers

The unit can failover if one of the following events occurs:

- An administrator manually switches over from active to standby.
- The standby Cisco ASA stops receiving keepalive packets on the failover command interface.
- The command interface link goes down.
- The link state of an interface goes down.
- The unit has a hardware failure or a power failure.
- The unit has a software failure.
- Too many monitored interfaces fail.
- The **no failover active** command is entered on the active unit, or the **failover active** command is entered on the standby unit.

Configuration Synchronization

Configuration synchronization occurs when one or both devices in the failover pair boot. Configurations are always synchronized from the active unit to the standby unit. When the standby unit completes its initial startup, it clears its running configuration (except for the failover commands needed to communicate with the active unit), and the active unit sends its entire configuration to the standby unit.

The following commands are replicated to the standby unit:

- all configuration commands except for the **mode**, **firewall**, and **failover lan unit** commands
- **copy running-config startup-config**

- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

The following commands are not replicated to the standby unit:

- all forms of the **copy** command except for **copy running-config startup-config**
- all forms of the **write** command except for **write memory**
- **debug**
- **failover lan unit**
- **firewall**
- **mode**
- **show**

Passage of State Information to the Standby Unit

The standby ASA monitors the status of the active ASA by sending keepalive messages over a dedicated Gigabit Ethernet failover connection between the two (also known as LAN-based failover). The active also does the reverse to the standby ASA.This failover design is stateful, which means that the active ASA maintains the connection table and replicates it to the standby ASA. Whenever there is a change in the table, the active ASA sends a stateful update to the standby.

The state information passed to the standby unit includes the following:

- NAT translation table
- TCP connection states
- UDP connection states
- ARP table
- Layer 2 bridge table (when running in transparent firewall mode)
- HTTP connection states (if HTTP replication is enabled)
- ISAKMP and IPsec SA table
- GTP PDP connection database

The information that is not passed to the standby unit when stateful failover is enabled includes the following:

- HTTP connection table (unless HTTP replication is enabled)
- User authentication (uauth) table
- Routing tables
- State information for security service modules
- DHCP server address leases
- L2TP over IPsec state information

Active/Standby Failover Configuration

Note Before configuring the failover, verify that the second Cisco ASA is turned off. Also verify that the activation key on the Cisco ASA supports failover and both Cisco ASAs are using the same mode (single or multiple).

Selecting the Failover Link

The first step is to decide which interface will be used to send failover control messages. The failover control link interface is defined by using the **failover lan interface** command followed by the interface name. The following example shows that the Cisco ASA is using GigabitEthernet0/2 as the failover control interface. In this example, the LAN interface is given a name of *FOCtrlIntf*. However, you can specify any name for this interface.

```
Chicago(config)# failover lan interface FOCtrlIntf GigabitEthernet0/2
```

Note If an interface already has the **nameif** statement configured, the security Cisco ASA displays an error stating that the interface is already in use. For example:

```
Chicago(config)# failover lan interface FOCtrlIntf GigabitEthernet0/2
interface already in use
```

To fix this issue, issue the **no nameif** command under that interface.

After the **failover lan interface** command is configured, the Cisco ASA adds a description under the failover interface configuration. It also clears any configuration parameters on that interface, as follows:

```
Chicago# show running | begin interface GigabitEthernet0/2
interface GigabitEthernet0/2
    description LAN failover Interface
```

Assigning Failover IP Addresses

After selecting which failover control interface the Cisco ASA is going to use, the next step is to configure the physical interfaces for the system and the standby IP addresses. The active Cisco ASA uses the system IP addresses, while the standby Cisco ASA uses the standby IP addresses. The following example shows that the Chicago Cisco ASA is using 209.165.200.225 and 192.168.10.1 as the system IP addresses, and 209.165.200.226 and 192.168.10.2 as the failover IP addresses on the outside and inside interfaces, respectively.

```
Chicago(config)# interface GigabitEthernet0/0
Chicago(config-if)# nameif outside
Chicago(config-if)# security-level 0
Chicago(config-if)# ip address 209.165.200.225 255.255.255.224 standby 209.165.200.226
Chicago(config-if)# exit
Chicago(config)# interface GigabitEthernet0/1
Chicago(config-if)# nameif inside
Chicago(config-if)# security-level 100
Chicago(config-if)# ip address 192.168.10.1 255.255.255.0 standby 192.168.10.2
```

For two security Cisco ASAs to communicate, the designated failover control interface should be configured with an IP address as well. Following is the complete command syntax to configure an IP address on the failover control interface:

failover interface ip *interface_name ip_address mask* **standby** *ip_address*

interface_name is the designated interface used for failover. The first IP address is the interface IP address used by the active Cisco ASA, and the second IP address is the IP address used by the standby Cisco ASA. The active unit uses its address to synchronize the running configuration with the standby. In the following example, the active Cisco ASA is assigned a 10.10.10.1 IP address along with a standby IP address of 10.10.10.2.

```
Chicago# configure terminal
Chicago(config)# failover interface ip FOCtrlIntf 10.10.10.1 255.255.255.252 standby
10.10.10.2
```

Setting Failover Key (Optional)

To secure the failover control messages sent between the Cisco ASAs, an administrator can optionally specify a shared secret key. The shared secret key encrypts and authenticates the failover messages if they are susceptible to unauthorized users. The following example shows how to configure a failover shared secret key of *cisco123*.

```
Chicago# configure terminal
Chicago(config)# failover key cisco123
```

The failover key uses DES or AES, depending on the installed license. It also uses MD5 as the hash to authenticate the message. Therefore, it is important that both Cisco ASAs use the same cipher license key.

Note If a failover key is not used, the active Cisco ASA sends all information in clear text, including the UDP/TCP states, the user credentials, and the VPN-related information.

Designating the Primary Cisco ASA

The two security Cisco ASAs send failover control messages through a network cable that has identical ends. Unlike a Cisco PIX firewall, in which the failover cable decides which firewall becomes primary, it is impossible to designate a Cisco ASA as primary based on the cable. To resolve the problem of which device should act as primary or secondary, you must designate the primary and secondary status through software configuration by using the **failover lan unit** command. In the following example, FO1 is designated as the primary failover Cisco ASA.

```
Chicago# configure terminal
Chicago(config)# failover lan unit primary
```

Enabling Stateful Failover (Optional)

As discussed earlier, the stateful failover feature in the Cisco ASA replicates the state and translation tables from the active unit to the standby unit. In the event of a failure, the standby unit takes over the connections, and data flows are not interrupted. The stateful failover requires a network interface to replicate the states. Cisco ASA can use either a dedicated or the failover control interface to replicate the updates. A stateful link interface is defined by using the **failover link** command followed by the

name of the interface. In the following example, the primary Cisco ASA is using GigabitEthernet0/3 as the stateful interface. The interface IP is 10.10.10.5 and the standby IP address is 10.10.10.6. The administrator uses *statefullink* as the interface name.

```
Chicago(config)# failover link statefullink GigabitEthernet0/3
Chicago(config)# failover interface ip statefullink 10.10.10.5 255.255.255.252 standby
10.10.10.6
```

Note Like the **failover lan interface** command, the Cisco ASA adds a description under the stateful link interface and clears any configuration on that interface.

For stateful failover, you can use the failover LAN interface if the stateful updates do not oversubscribe the interface bandwidth. Set up a different interface for stateful failover if you are concerned about possibly oversubscribing the failover control interface. If the security Cisco ASA uses the same interface for both control and stateful messages, you have to connect the security Cisco ASA through a switch. Crossover cable is not supported.

The stateful failover does not replicate HTTP-based connections. HTTP connections usually have a short lifetime and therefore are not replicated by default. Additionally, they add considerable load on the security Cisco ASA if the amount of HTTP traffic is large in comparison to other traffic.

If the HTTP connections need to be replicated to the standby Cisco ASA, use the **failover replication http** command, as shown by the following example:

```
Chicago(config)# failover replication http
```

Enabling Failover Globally

The last step in configuring failover on the primary Cisco ASA is to enable failover globally. The following example shows how to enable failover in the Chicago FO1 Cisco ASA:

```
Chicago(config)# failover
```

Configuring Failover on the Secondary Cisco ASA

In the Cisco failover feature, there is no need to manually configure the secondary Cisco ASA. Instead, you just need to configure some basic information about failover. After that, the primary/active Cisco ASA starts synchronizing its configuration. The bootstrap configuration includes the following five configuration parameters:

- Failover designation
- Failover link interface
- Failover interface IP address
- Failover shared key
- Failover enable

The following example shows the bootstrap configuration of the secondary Cisco ASA needed in LAN-based failover:

```
failover lan unit secondary
failover lan interface FOCtrlIntf GigabitEthernet0/2
failover key cisco123
failover interface ip FOCtrlIntf 10.10.10.1 255.255.255.252 standby 10.10.10.2 failover
```

Note After failover is enabled on both Cisco ASAs, their running configuration is identical except for the **failover lan unit** command.

For a detailed explanation of configuring the ASA redundancy, see the following URL:
http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_chapter09186a008063b31a.html#wp1058096