Newer Design Guide Available

Cisco Smart Business Architecture has become part of the Cisco Validated Designs program.

For up-to-date guidance on the designs described in this guide, see http://cvddocs.com/fw/Aug13-505

For information about the Cisco Validated Design program, go to http://www.cisco.com/go/cvd

Data Center Configuration Files Guide

SMART BUSINESS ARCHITECTURE

February 2013 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in February 2013 is the "February Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide

Cisco SBA Data Center

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Data Center is a comprehensive design that scales from a server room to a data center for networks with up to 10,000 connected users. This design incorporates compute resources, security, application resiliency, and virtualization.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

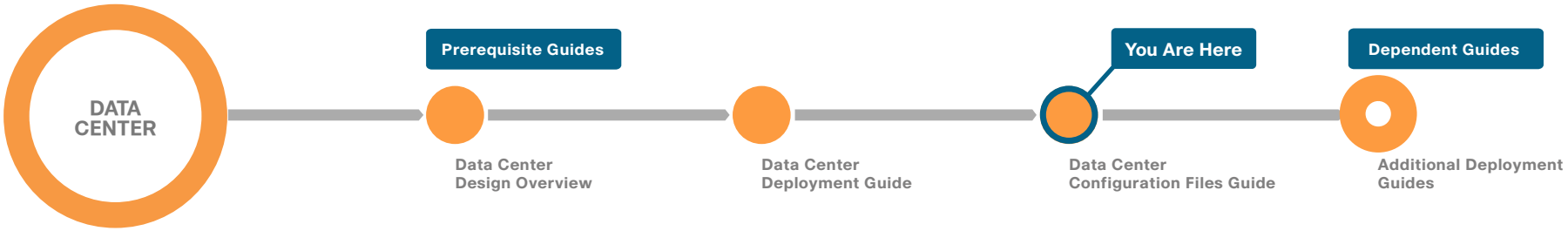
About This Guide

This *configuration files guide* provides, as a comprehensive reference, the complete network device configurations that are implemented in a Cisco SBA deployment guide.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel



Introduction

For our partners and customers with up to 10,000 connected users, Cisco has designed an out-of–the-box deployment that is simple, fast, affordable, scalable, and flexible. We have designed it to be easy—easy to configure, deploy, and manage.

The simplicity of this deployment, though, masks the depth and breadth of the architecture. Based on feedback from many customers and partners, Cisco has developed a solid network foundation with a flexible platform that does not require re-engineering to support additional network or user services.

For Cisco partners and customers whose data center will have up to 300 ports with a mix of physical or virtual servers, Cisco has created a data center architecture that is flexible, scalable, reliable, and affordable. The step-by-step guidance in the data center deployment guides makes it easy to install, configure, and manage, which reduces the time and cost needed to deploy your data center.

By building on to the foundation LAN and WAN architecture you've already deployed with the Cisco Smart Business Architecture (SBA) Borderless Network Foundation, the SBA data center lets you migrate from your current server room without wasting time and expense reconfiguring your existing network foundation.

The following configuration files are provided:

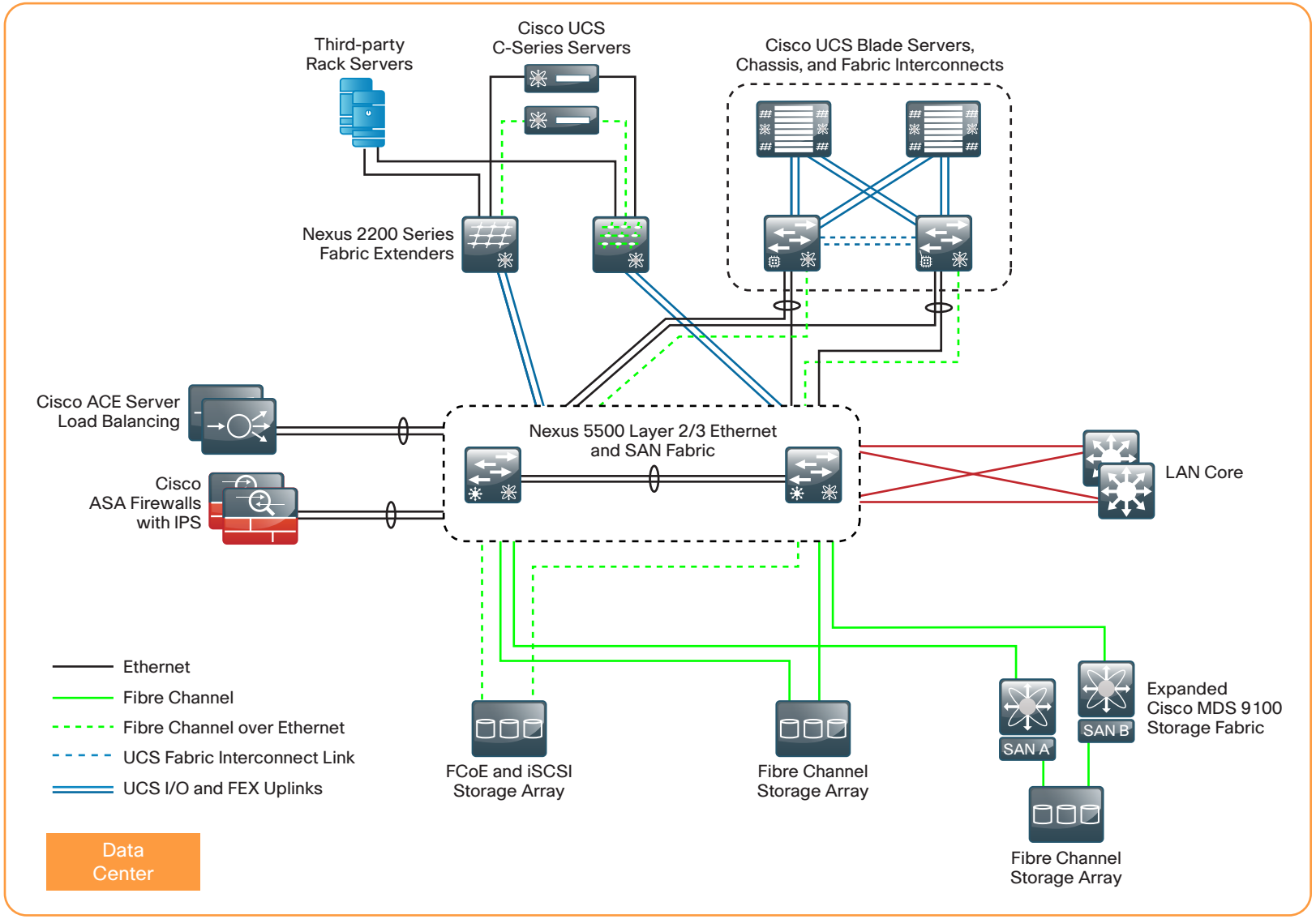
- Data Center Ethernet and Fibre Channel Infrastructure
- Data Center Network Security
- Data Center Application Resilience

Refer to Appendix A for a complete list of products used in the lab testing of this design.

Figure 1 illustrates the complete Cisco SBA data center architecture.

Notes

Figure 1 - Cisco SBA data center architecture



Data Center Ethernet and Fibre Channel Infrastructure

This section includes the Cisco Nexus 5500UP Series switches, used to build out the data center core Ethernet and Fibre Channel switching foundation, and the Cisco MDS 9100 Multilayer Fabric switches, used to extend your Fibre Channel networks for larger density requirements. For the Cisco SBA February 2013 Series, we used the Cisco Nexus 5596 model switch with Universal Port capability; however, the configurations would be the same for a Cisco Nexus 5548 except for the number of ports available.

Cisco Nexus 5596UPa

The Cisco Nexus 5500UP switches operate as a pair to provide a resilient data center core for both Ethernet and Fibre Channel network transport. This switch is also the Fibre Channel SAN-A switch.

```
version 5.2(1)N1(1b)
feature fcoe
logging level feature-mgr 0
hostname DC5596UPa
feature npiv
feature fport-channel-trunk
no feature telnet
feature tacacs+
cfs eth distribute
feature pim
feature eigrp
feature udld
feature interface-vlan
feature hsrp
feature lacp
feature vpc
feature lldp
feature fex
username admin password 5 ***** role network-admin
banner motd #Nexus 5000 Switch
#
ssh key rsa 2048
ip domain-lookup
ip name-server 10.4.48.10
tacacs-server host 10.4.48.15 key 7 *****
aaa group server tacacs+ tacacs
    server 10.4.48.15
    source-interface loopback0
ip access-list ISCSI
  10 permit tcp any eq 860 any
  20 permit tcp any eq 3260 any
  30 permit tcp any any eq 860
  40 permit tcp any any eq 3260
class-map type qos class-fcoe
class-map type qos match-any BULK-COS
  match cos 1
class-map type qos match-any BULK-QUEUE
  match dscp 10,12,14
  match cos 1
class-map type qos match-any CONTROL-COS
  match cos 4
class-map type qos match-all ISCSI-QUEUE
  match access-group name ISCSI
class-map type qos match-any PRIORITY-COS
  match cos 5
class-map type qos match-any CONTROL-QUEUE
  match dscp 24
  match cos 4
class-map type qos match-any PRIORITY-QUEUE
  match dscp 32,34,40,46
  match cos 5
class-map type qos match-any TRANSACTIONAL-COS
  match cos 2
```

```
class-map type qos match-any TRANSACTIONAL-QUEUE
  match dscp 18,20,22
  match cos 2
class-map type queuing BULK-GROUP
  match qos-group 3
class-map type queuing class-fcoe
  match qos-group 1
class-map type queuing CONTROL-GROUP
  match qos-group 4
class-map type queuing PRIORITY-GROUP
  match qos-group 5
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
class-map type queuing TRANSACTIONAL-GROUP
  match qos-group 2
policy-map type qos DC-FCOE+1P4Q_GLOBAL-COS-QOS
  class PRIORITY-COS
    set qos-group 5
  class CONTROL-COS
    set qos-group 4
  class class-fcoe
    set qos-group 1
  class TRANSACTIONAL-COS
    set qos-group 2
  class BULK-COS
    set qos-group 3
  class class-default
policy-map type qos DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  class PRIORITY-QUEUE
    set qos-group 5
  class CONTROL-QUEUE
    set qos-group 4
  class TRANSACTIONAL-QUEUE
    set qos-group 2
  class BULK-QUEUE
    set qos-group 3
  class ISCSI-QUEUE
    set qos-group 3
  class class-default
policy-map type queuing DC-FCOE+1P4Q_GLOBAL-GROUP-QUEUING
  class type queuing PRIORITY-GROUP
    priority
  class type queuing CONTROL-GROUP
    bandwidth percent 10
  class type queuing class-fcoe
    bandwidth percent 20
  class type queuing TRANSACTIONAL-GROUP
    bandwidth percent 25
  class type queuing BULK-GROUP
    bandwidth percent 20
  class type queuing class-default
    bandwidth percent 25
class-map type network-qos class-fcoe
  match qos-group 1
class-map type network-qos BULK-SYSTEM
  match qos-group 3
class-map type network-qos CONTROL-SYSTEM
  match qos-group 4
class-map type network-qos PRIORITY-SYSTEM
  match qos-group 5
class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
class-map type network-qos TRANSACTIONAL-SYSTEM
  match qos-group 2
policy-map type network-qos DC-FCOE+1P4Q_GLOBAL-SYSTEM-NETWORK-
QOS
  class type network-qos PRIORITY-SYSTEM
    set cos 5
  class type network-qos CONTROL-SYSTEM
    set cos 4
```

```
  class type network-qos class-fcoe
    pause no-drop
    mtu 2158
  class type network-qos TRANSACTIONAL-SYSTEM
    set cos 2
  class type network-qos BULK-SYSTEM
    mtu 9216
    queue-limit 128000 bytes
    set cos 1
  class type network-qos class-default
    multicast-optimize
    set cos 0
system qos
  service-policy type qos input DC-FCOE+1P4Q_GLOBAL-COS-QOS
  service-policy type queuing input DC-FCOE+1P4Q_GLOBAL-GROUP-
QUEUING
  service-policy type queuing output DC-FCOE+1P4Q_GLOBAL-GROUP-
QUEUING
  service-policy type network-qos DC-FCOE+1P4Q_GLOBAL-SYSTEM-
NETWORK-QOS
fex 100
  pinning max-links 1
  description "FEX0100"
fex 103
  pinning max-links 1
  description "FEX0103"
fex 104
  pinning max-links 1
  description "FEX0104"
fex 106
  pinning max-links 1
  description "FEX0106"
fex 107
  pinning max-links 1
  description "FEX0107"
slot 1
  port 43-48 type fc
snmp-server user admin network-admin auth md5 ***** localizedkey
snmp-server host 10.4.48.30 traps version 2c public  udp-port
2162
snmp-server host 10.4.63.200 traps version 2c public  udp-port
1163
snmp-server community ***** group network-operator
snmp-server community ***** group network-admin
ntp server 10.4.48.17 use-vrf management
aaa authentication login default group tacacs
vrf context management
  ip route 0.0.0.0/0 10.4.63.1
track 1 interface port-channel10 line-protocol
track 2 interface Ethernet1/19 line-protocol
track 3 interface Ethernet1/20 line-protocol
track 10 list boolean or
  object 1
  object 2
  object 3
vlan 1
vlan 116
  name WLAN_Data
vlan 120
  name WLAN_Voice
vlan 146
  name WLAN_Mgmt
vlan 148
  name Servers_1
vlan 149
  name Servers_2
vlan 150
  name Servers_3
vlan 153
  name FW_Outside
vlan 154
  name FW_Inside_1
vlan 155
  name FW_Inside_2
```

```
vlan 156
  name PEERING_VLAN
vlan 160
  name 1kv-Control
vlan 161
  name vMotion
vlan 162
  name iSCSI
vlan 163
  name DC-Management
vlan 304
  fcoe vsan 4
vlan 912
  name ACE-Heartbeat
spanning-tree vlan 1-400 priority 8192
route-map static-to-eigrp permit 10
  match ip address 10.4.54.0/24
route-map static-to-eigrp permit 20
  match ip address 10.4.55.0/24
port-channel load-balance ethernet source-dest-port
vpc domain 10
  peer-switch
  role priority 16000
  peer-keepalive destination 10.4.63.11 source 10.4.63.10
  delay restore 360
  peer-gateway
  track 10
  auto-recovery
  ip arp synchronize
port-profile default max-ports 512

vsan database
  vsan 4 name "General-Storage"
device-alias database
  device-alias name emc-a1-p0-fc pwwn 50:06:01:60:47:20:2e:b7
  device-alias name emc-b1-p1-fc pwwn 50:06:01:69:47:20:2e:b7
device-alias commit

fcdomain fcid database
  vsan 4 wwn 50:06:01:64:47:20:2e:b7 fcid 0x5a0000 dynamic
  vsan 4 wwn 50:06:01:6d:47:20:2e:b7 fcid 0x5a0020 dynamic
  vsan 4 wwn 24:1d:54:7f:ee:7b:54:00 fcid 0x5a0040 dynamic
  vsan 4 wwn 20:1f:54:7f:ee:7b:54:00 fcid 0x5a0060 dynamic
  vsan 4 wwn 20:20:54:7f:ee:7b:54:00 fcid 0x5a0080 dynamic
  vsan 4 wwn 20:ff:00:25:b5:0a:00:7f fcid 0x5a0041 dynamic

interface Vlan1

interface Vlan116
  no shutdown
  description Wireless Data Network
  no ip redirects
  ip address 10.4.16.2/22
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 116
    priority 110
    ip 10.4.16.1

interface Vlan120
  no shutdown
  description Wireless Voice Network
  no ip redirects
  ip address 10.4.20.2/22
  ip router eigrp 100
  ip passive-interface eigrp 100
  hsrp 120
    priority 110
    ip 10.4.20.1

interface Vlan146
  no shutdown
  description Wireless Management Network
```

```
  no ip redirects
  ip address 10.4.46.2/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 146
    priority 110
    ip 10.4.46.1

interface Vlan148
  no shutdown
  description Servers_1
  no ip redirects
  ip address 10.4.48.2/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 148
    priority 110
    ip 10.4.48.1

interface Vlan149
  no shutdown
  description Servers_2
  no ip redirects
  ip address 10.4.49.2/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 149
    priority 110
    ip 10.4.49.1

interface Vlan150
  no shutdown
  description Servers_3
  no ip redirects
  ip address 10.4.50.2/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 150
    priority 110
    ip 10.4.50.1

interface Vlan153
  no shutdown
  description FW_Outside
  no ip redirects
  ip address 10.4.53.2/25
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 153
    priority 110
    ip 10.4.53.1

interface Vlan156
  no shutdown
  ip address 10.4.56.1/30
  ip router eigrp 100
  ip pim sparse-mode

interface Vlan162
  no shutdown
  description iSCSI VLAN
  no ip redirects
  ip address 10.4.62.2/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  hsrp 162
    priority 110
    ip 10.4.62.1
```

```
interface Vlan163
  no shutdown
  description DC-Management
  no ip redirects
  ip address 10.4.63.2/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  hsrp 163
    priority 110
    ip 10.4.63.1

interface san-port-channel 1
  switchport mode E
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 4

interface san-port-channel 29
  channel mode active
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 4
  switchport trunk mode on

interface port-channel10
  description vPC Peer-Link
  switchport mode trunk
  spanning-tree port type network
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc peer-link

interface port-channel21
  description Link to Management Switch for VLAN 163
  switchport mode trunk
  switchport trunk allowed vlan 163
  speed 1000
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc 21

interface port-channel50
  switchport mode trunk
  switchport trunk allowed vlan 148-163
  spanning-tree port type edge trunk
  speed 10000
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc 50

interface port-channel51
  switchport mode trunk
  switchport trunk allowed vlan 148-163
  spanning-tree port type edge trunk
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  speed 10000
  vpc 51

interface port-channel53
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  speed 10000
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc 53

interface port-channel54
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  speed 10000
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc 54

interface port-channel67
  description Link to WLC5508-1 {P1 & P2}
  switchport mode trunk
  switchport trunk allowed vlan 116,120,146
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS

interface port-channel68
```

```
  description Link to WLC5508-2 {P1 & P2}
  switchport mode trunk
  switchport trunk allowed vlan 116,120,146
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS

interface port-channel100
  description Dual-Homed 2248TP FEX
  switchport mode fex-fabric
  fex associate 100
  vpc 100

interface port-channel103
  description Dual-Homed 2232PP FEX
  switchport mode fex-fabric
  fex associate 103
  vpc 103

interface port-channel104
  description Dual-Homed 2232PP FEX
  switchport mode fex-fabric
  fex associate 104
  vpc 104

interface port-channel106
  description Dual-Homed 2248 TP-E
  switchport mode fex-fabric
  fex associate 106
  vpc 106

interface port-channel107
  description Dual-Homed 2248 TP-E
  switchport mode fex-fabric
  fex associate 107
  vpc 107

interface vfc27
  bind interface Ethernet1/27
  switchport description Link to EMC(VNX5700)SlotA2-P0{FCoE}
  no shutdown

interface vfc28
  bind interface Ethernet1/28
  switchport description Link to EMC (VNX5700) SlotB2-P1
  no shutdown
vsan database
  vsan 4 interface vfc27
  vsan 4 interface vfc28
  vsan 4 interface san-port-channel 29

interface fc1/43

interface fc1/44

interface fc1/45
  switchport trunk mode on
  channel-group 29 force
  no shutdown

interface fc1/46
  switchport trunk mode on
  channel-group 29 force
  no shutdown

interface fc1/47
  channel-group 1 force
  no shutdown

interface fc1/48
  channel-group 1 force
  no shutdown

interface Ethernet1/1
  description DC5585a Ten0/8
  switchport mode trunk
```

```
  switchport trunk allowed vlan 153-155
  channel-group 53 mode active

interface Ethernet1/2
  description DC5585b Ten0/8
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  channel-group 54 mode active

interface Ethernet1/3
  description ACE 1 Gig 1/1
  switchport mode trunk
  switchport trunk allowed vlan 149,912
  speed 1000
  channel-group 13
  vpc orphan-port suspend

interface Ethernet1/4
  description ACE 1 Gig 1/2
  switchport mode trunk
  switchport trunk allowed vlan 149,912
  speed 1000
  channel-group 13
  vpc orphan-port suspend

interface Ethernet1/5
  switchport mode fex-fabric
  fex associate 106
  channel-group 106

interface Ethernet1/6
  switchport mode fex-fabric
  fex associate 106
  channel-group 106

interface Ethernet1/7
  switchport mode fex-fabric
  fex associate 107
  channel-group 107

interface Ethernet1/8
  switchport mode fex-fabric
  fex associate 107
  channel-group 107

interface Ethernet1/9
  description Link to FI-A Eth 1/17
  switchport mode trunk
  switchport trunk allowed vlan 148-163
  channel-group 50 mode active

interface Ethernet1/10
  description Link to FI-A Eth 1/18
  switchport mode trunk
  switchport trunk allowed vlan 148-163
  channel-group 50 mode active

interface Ethernet1/11
  description Link to FI-B Eth 1/17
  switchport mode trunk
  switchport trunk allowed vlan 148-163
  channel-group 51 mode active

interface Ethernet1/12
  description Link to FI-B Eth 1/18
  switchport mode trunk
  switchport trunk allowed vlan 148-163
  channel-group 51 mode active

interface Ethernet1/13
  description Dual-Homed 2248TP FEX
  switchport mode fex-fabric
  fex associate 100
  channel-group 100
```

```
interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17
  description vPC Peer-Link
  switchport mode trunk
  channel-group 10 mode active

interface Ethernet1/18
  description vPC Peer-Link
  switchport mode trunk
  channel-group 10 mode active

interface Ethernet1/19
  description Link to Core-1
  no switchport
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  ip address 10.4.40.50/30
  ip router eigrp 100
  ip pim sparse-mode

interface Ethernet1/20
  description Link to Core-2
  no switchport
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  ip address 10.4.40.54/30
  ip router eigrp 100
  ip pim sparse-mode

interface Ethernet1/21
  description Link to Management Switch for VLAN 163
  switchport mode trunk
  switchport trunk allowed vlan 163
  speed 1000
  channel-group 21 mode active

interface Ethernet1/22

interface Ethernet1/23
  description Dual-Homed 2232PP FEX
  switchport mode fex-fabric
  fex associate 103
  channel-group 103

interface Ethernet1/24
  description Dual-Homed 2232PP FEX
  switchport mode fex-fabric
  fex associate 103
  channel-group 103

interface Ethernet1/25
  description Dual-Homed 2232PP FEX
  switchport mode fex-fabric
  fex associate 104
  channel-group 104

interface Ethernet1/26
  description Dual-Homed 2232PP FEX
  switchport mode fex-fabric
  fex associate 104
  channel-group 104

interface Ethernet1/27
  description Link to EMC (VNX5700) SlotA2-P0
  switchport mode trunk
  switchport trunk allowed vlan 304
  spanning-tree port type edge trunk

interface Ethernet1/28
  description Link to EMC (VNX5700) SlotB2-P1
```

```
  switchport mode trunk
  switchport trunk allowed vlan 304
  spanning-tree port type edge trunk

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface Ethernet1/33

interface Ethernet1/34

interface Ethernet1/35

interface Ethernet1/36

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet1/41

interface Ethernet1/42

interface mgmt0
  ip address 10.4.63.10/24

interface loopback0
  ip address 10.4.56.254/32
  ip router eigrp 100
  ip pim sparse-mode

interface Ethernet103/1/1
  description Links to 7500-1 {Ten0/0/1}
  switchport mode trunk
  switchport trunk allowed vlan 146
 service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS

interface Ethernet103/1/2
  description link to 7500-2
  switchport mode trunk
  switchport trunk allowed vlan 146
 service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS

interface Ethernet103/1/3

!************************************************
! interfaces Ethernet103/1/4 to 103/1/31 are not
! configured and have been removed for brevity
!************************************************

interface Ethernet103/1/32

interface Ethernet104/1/1
  description link to 7500-1 (Ten0/0/1)
  switchport mode trunk
  switchport trunk allowed vlan 146
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS

interface Ethernet104/1/2
  description link to 7500-2
  switchport mode trunk
  switchport trunk allowed vlan 146
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS

interface Ethernet104/1/3
```

```
!************************************************
! interfaces Ethernet104/1/4 to 104/1/31 are not
! configured and have been removed for brevity
!************************************************

interface Ethernet104/1/32

interface Ethernet106/1/1
  description Link to WLC5508-1 (P1)
  switchport mode trunk
  switchport trunk allowed vlan 116,120,146
  channel-group 67

interface Ethernet106/1/2
  description Link to WLC5508-1 (P2)
  switchport mode trunk
  switchport trunk allowed vlan 116,120,146
  channel-group 67

interface Ethernet106/1/3
  switchport access vlan 148
  spanning-tree port type edge
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS

interface Ethernet106/1/4

!************************************************
! interfaces Ethernet106/1/5 to 106/1/45 are not
! configured and have been removed for brevity
!************************************************

interface Ethernet106/1/46

interface Ethernet106/1/47
  description LAB VPN Access
  switchport access vlan 148
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS

interface Ethernet106/1/48
  description Connected to Backend ESX Server
  switchport mode trunk
  switchport trunk native vlan 148
  switchport trunk allowed vlan 148-163
  spanning-tree port type edge trunk
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS

interface Ethernet107/1/1
  description Link to WLC5508-2 (P1)
  switchport mode trunk
  switchport trunk allowed vlan 116,120,146
  channel-group 68

interface Ethernet107/1/2
  description Link to WLC5508-2 (P2)
  switchport mode trunk
  switchport trunk allowed vlan 116,120,146
  channel-group 68

interface Ethernet107/1/3

interface Ethernet107/1/4

!************************************************
! interfaces Ethernet107/1/5 to 107/1/45 are not
! configured and have been removed for brevity
!************************************************

interface Ethernet107/1/46

interface Ethernet107/1/47
  description NTP Server
  switchport access vlan 148
  spanning-tree port type edge
```

```
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS

interface Ethernet107/1/48
  description Openfiler
  switchport access vlan 148
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS

clock timezone PST -8 0
clock summer-time PDT 2 Sunday march 02:00 1 Sunday nov 02:00 60
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.2.1.N1.1b.bin
boot system bootflash:/n5000-uk9.5.2.1.N1.1b.bin
router eigrp 100
  router-id 10.4.56.254
  redistribute static route-map static-to-eigrp
ip route 10.4.54.0/24 Vlan153 10.4.53.126
ip route 10.4.55.0/24 Vlan153 10.4.53.126
ip pim ssm range 232.0.0.0/8
ip pim auto-rp forward listen
no ip igmp snooping mrouter vpc-peer-link
vpc bind-vrf default vlan 900
interface fc1/45
interface fc1/46
interface fc1/47
interface fc1/48
interface fc1/43
interface fc1/44
interface fc1/45
interface fc1/46
interface fc1/47
  switchport mode E
interface fc1/48
  switchport mode E
zoneset distribute full vsan 4
!Full Zone Database Section for vsan 4
zone name p29-ucs-b-fc0-ch1s3_emc vsan 4
    member pwwn 50:06:01:60:47:20:2e:b7
!               [emc-a1-p0-fc]
    member pwwn 50:06:01:69:47:20:2e:b7
!               [emc-b1-p1-fc]
    member pwwn 20:ff:00:25:b5:0a:00:7f

zoneset name SAN_4 vsan 4
    member p29-ucs-b-fc0-ch1s3_emc

zoneset activate name SAN_4 vsan 4
```

Cisco Nexus 5596UPb

The Cisco Nexus 5500UP switches operate as a pair to provide a resilient data center core for both Ethernet and Fibre Channel network transport. This switch is also the Fibre Channel SAN-B switch.

```
version 5.2(1)N1(1b)
feature fcoe
logging level feature-mgr 0
hostname DC5596UPb
feature npiv
feature fport-channel-trunk
no feature telnet
feature tacacs+
cfs eth distribute
feature pim
feature eigrp
feature udld
feature interface-vlan
feature hsrp
feature lacp
feature vpc
feature lldp
feature fex
username admin password 5 ***** role network-admin
banner motd #Nexus 5000 Switch
#
```

```
ssh key rsa 2048
ip domain-lookup
tacacs-server host 10.4.48.15 key 7 *****
aaa group server tacacs+ tacacs
    server 10.4.48.15
    source-interface loopback0
logging event link-status default
ip access-list ISCSI
  10 permit tcp any eq 860 any
  20 permit tcp any eq 3260 any
  30 permit tcp any any eq 860
  40 permit tcp any any eq 3260
class-map type qos class-fcoe
class-map type qos match-any BULK-COS
  match cos 1
class-map type qos match-any BULK-QUEUE
  match dscp 10,12,14
  match cos 1
class-map type qos match-any CONTROL-COS
  match cos 4
class-map type qos match-all ISCSI-QUEUE
  match access-group name ISCSI
class-map type qos match-any PRIORITY-COS
  match cos 5
class-map type qos match-any CONTROL-QUEUE
  match dscp 24
  match cos 4
class-map type qos match-any PRIORITY-QUEUE
  match dscp 32,34,40,46
  match cos 5
class-map type qos match-any TRANSACTIONAL-COS
  match cos 2
class-map type qos match-any TRANSACTIONAL-QUEUE
  match dscp 18,20,22
  match cos 2
class-map type queuing BULK-GROUP
  match qos-group 3
class-map type queuing class-fcoe
  match qos-group 1
class-map type queuing CONTROL-GROUP
  match qos-group 4
class-map type queuing PRIORITY-GROUP
  match qos-group 5
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
class-map type queuing TRANSACTIONAL-GROUP
  match qos-group 2
policy-map type qos DC-FCOE+1P4Q_GLOBAL-COS-QOS
  class PRIORITY-COS
    set qos-group 5
  class CONTROL-COS
    set qos-group 4
  class class-fcoe
    set qos-group 1
  class TRANSACTIONAL-COS
    set qos-group 2
  class BULK-COS
    set qos-group 3
  class class-default
policy-map type qos DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  class PRIORITY-QUEUE
    set qos-group 5
  class CONTROL-QUEUE
    set qos-group 4
  class TRANSACTIONAL-QUEUE
    set qos-group 2
  class BULK-QUEUE
    set qos-group 3
  class ISCSI-QUEUE
    set qos-group 3
  class class-default
policy-map type queuing DC-FCOE+1P4Q_GLOBAL-GROUP-QUEUING
```

```
  class type queuing PRIORITY-GROUP
    priority
  class type queuing CONTROL-GROUP
    bandwidth percent 10
  class type queuing class-fcoe
    bandwidth percent 20
  class type queuing TRANSACTIONAL-GROUP
    bandwidth percent 25
  class type queuing BULK-GROUP
    bandwidth percent 20
  class type queuing class-default
    bandwidth percent 25
class-map type network-qos class-fcoe
  match qos-group 1
class-map type network-qos BULK-SYSTEM
  match qos-group 3
class-map type network-qos CONTROL-SYSTEM
  match qos-group 4
class-map type network-qos PRIORITY-SYSTEM
  match qos-group 5
class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
class-map type network-qos TRANSACTIONAL-SYSTEM
  match qos-group 2
policy-map type network-qos DC-FCOE+1P4Q_GLOBAL-SYSTEM-NETWORK-
QOS
  class type network-qos PRIORITY-SYSTEM
    set cos 5
  class type network-qos CONTROL-SYSTEM
    set cos 4
  class type network-qos class-fcoe
    pause no-drop
    mtu 2158
  class type network-qos TRANSACTIONAL-SYSTEM
    set cos 2
  class type network-qos BULK-SYSTEM
    mtu 9216
    queue-limit 128000 bytes
    set cos 1
  class type network-qos class-default
    multicast-optimize
    set cos 0
system qos
  service-policy type qos input DC-FCOE+1P4Q_GLOBAL-COS-QOS
  service-policy type queuing input DC-FCOE+1P4Q_GLOBAL-GROUP-
QUEUING
  service-policy type queuing output DC-FCOE+1P4Q_GLOBAL-GROUP-
QUEUING
  service-policy type network-qos DC-FCOE+1P4Q_GLOBAL-SYSTEM-
NETWORK-QOS
policy-map type control-plane copp-system-policy-customized
  class copp-system-class-default
    police cir 2048 kbps bc 6400000 bytes
fex 100
  pinning max-links 1
  description "FEX0100"
fex 103
  pinning max-links 1
  description "FEX0103"
fex 104
  pinning max-links 1
  description "FEX0104"
fex 106
  pinning max-links 1
  description "FEX0106"
fex 107
  pinning max-links 1
  description "FEX0107"
slot 1
  port 43-48 type fc
snmp-server user admin network-admin auth md5 ***** localizedkey
snmp-server host 10.4.48.30 traps version 2c public  udp-port
```

```
1164
snmp-server host 10.4.48.30 traps version 2c public  udp-port
2162
snmp-server community ***** group network-admin
snmp-server community ***** group network-operator
ntp server 10.4.48.17
aaa authentication login default group tacacs
vrf context management
  ip route 0.0.0.0/0 10.4.63.1
track 1 interface port-channel10 line-protocol
track 2 interface Ethernet1/19 line-protocol
track 3 interface Ethernet1/20 line-protocol
track 10 list boolean or
  object 1
  object 2
  object 3
vlan 1
vlan 116
  name WLAN_Data
vlan 120
  name WLAN_Voice
vlan 146
  name WLAN_Mgmt
vlan 148
  name Servers_1
vlan 149
  name Servers_2
vlan 150
  name Servers_3
vlan 153
  name FW_Outside
vlan 154
  name FW_Inside_1
vlan 155
  name FW_Inside_2
vlan 156
  name PEERING_VLAN
vlan 160
  name 1kv-Control
vlan 161
  name vMotion
vlan 162
  name iSCSI
vlan 163
  name DC-Management
vlan 305
  fcoe vsan 5
vlan 912
  name ACE-Heartbeat
spanning-tree vlan 1-400 priority 8192
route-map static-to-eigrp permit 10
  match ip address 10.4.54.0/24
route-map static-to-eigrp permit 20
  match ip address 10.4.55.0/24
port-channel load-balance ethernet source-dest-port
vpc domain 10
  peer-switch
  peer-keepalive destination 10.4.63.10 source 10.4.63.11
  delay restore 360
  peer-gateway
  track 10
  auto-recovery
  ip arp synchronize
port-profile default max-ports 512

vsan database
  vsan 5 name "General-Storage"
device-alias database
  device-alias name emc-a1-p1-fc pwwn 50:06:01:61:47:20:2e:b7
  device-alias name emc-b1-p0-fc pwwn 50:06:01:68:47:20:2e:b7
device-alias commit

fcdomain fcid database
  vsan 5 wwn 50:06:01:6c:47:20:2e:b7 fcid 0xa20000 dynamic
```

```
  vsan 5 wwn 50:06:01:65:47:20:2e:b7 fcid 0xa20020 dynamic
  vsan 5 wwn 20:1f:54:7f:ee:7b:53:40 fcid 0xa20040 dynamic
  vsan 5 wwn 20:20:54:7f:ee:7b:53:40 fcid 0xa20060 dynamic
  vsan 5 wwn 24:1d:54:7f:ee:7b:53:40 fcid 0xa20080 dynamic
  vsan 5 wwn 20:ff:00:25:b5:0b:00:7f fcid 0xa20081 dynamic


interface Vlan1

interface Vlan116
  no shutdown
  description Wireless Data Network
  no ip redirects
  ip address 10.4.16.3/22
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 116
    ip 10.4.16.1

interface Vlan120
  no shutdown
  description Wireless Voice Network
  no ip redirects
  ip address 10.4.20.3/22
  ip router eigrp 100
  ip passive-interface eigrp 100
  hsrp 120
    ip 10.4.20.1

interface Vlan146
  no shutdown
  description Wireless Management Network
  no ip redirects
  ip address 10.4.46.3/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 146
    ip 10.4.46.1

interface Vlan148
  no shutdown
  description Servers_1
  no ip redirects
  ip address 10.4.48.3/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 148
    ip 10.4.48.1

interface Vlan149
  no shutdown
  description Servers_2
  no ip redirects
  ip address 10.4.49.3/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 149
    ip 10.4.49.1

interface Vlan150
  no shutdown
  description Servers_3
  no ip redirects
  ip address 10.4.50.3/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 150
    ip 10.4.50.1
```

```
interface Vlan153
  no shutdown
  description FW_Outside
  no ip redirects
  ip address 10.4.53.3/25
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 153
    ip 10.4.53.1

interface Vlan156
  no shutdown
  ip address 10.4.56.2/30
  ip router eigrp 100
  ip pim sparse-mode

interface Vlan162
  no shutdown
  description iSCSI VLAN
  no ip redirects
  ip address 10.4.62.3/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  hsrp 162
    ip 10.4.62.1

interface Vlan163
  no shutdown
  description DC-Management
  no ip redirects
  ip address 10.4.63.3/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  hsrp 163
    ip 10.4.63.1
```

```
interface san-port-channel 1
  switchport mode E
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 5

interface san-port-channel 29
  channel mode active
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 5
  switchport trunk mode on

interface port-channel10
  description vPC Peer-Link
  switchport mode trunk
  spanning-tree port type network
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc peer-link

interface port-channel21
  description Link to Management Switch for VLAN 163
  switchport mode trunk
  switchport trunk allowed vlan 163
  speed 1000
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc 21

interface port-channel50
  switchport mode trunk
  switchport trunk allowed vlan 148-163
  spanning-tree port type edge trunk
  speed 10000
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc 50

interface port-channel51
  switchport mode trunk
  switchport trunk allowed vlan 148-163
```

```
  spanning-tree port type edge trunk
  speed 10000
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc 51

interface port-channel53
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  speed 10000
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc 53

interface port-channel54
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  speed 10000
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc 54

interface port-channel67
  description Link to WLC5508-1 {P1 & P2}
  switchport mode trunk
  switchport trunk allowed vlan 116,120,146
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS

interface port-channel68
  description Link to WLC5508-2 {P1 & P2}
  switchport mode trunk
  switchport trunk allowed vlan 116,120,146
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS

interface port-channel100
  description Dual-Homed 2248TP FEX
  switchport mode fex-fabric
  fex associate 100
  vpc 100

interface port-channel103
  description Dual-Homed 2232PP FEX
  switchport mode fex-fabric
  fex associate 103
  vpc 103

interface port-channel104
  description Dual-Homed 2232PP FEX
  switchport mode fex-fabric
  fex associate 104
  vpc 104

interface port-channel106
  description Dual-Homed 2248 TP-E
  switchport mode fex-fabric
  fex associate 106
  vpc 106

interface port-channel107
  description Dual-Homed 2248 TP-E
  switchport mode fex-fabric
  fex associate 107
  vpc 107

interface vfc27
  bind interface Ethernet1/27
  switchport description Link to EMC(VNX5700)SlotB2-P0{FCoE}
  no shutdown

interface vfc28
  bind interface Ethernet1/28
  switchport description Link to EMC (VNX5700) SlotA2-P1
  no shutdown
vsan database
  vsan 5 interface vfc27
  vsan 5 interface vfc28
  vsan 5 interface san-port-channel 29
```

```
interface fc1/43

interface fc1/44

interface fc1/45
  switchport trunk mode on
  channel-group 29 force
  no shutdown

interface fc1/46
  switchport trunk mode on
  channel-group 29 force
  no shutdown

interface fc1/47
  channel-group 1 force
  no shutdown

interface fc1/48
  channel-group 1 force
  no shutdown

interface Ethernet1/1
  description DC5585a Ten0/9
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  channel-group 53 mode active

interface Ethernet1/2
  description DC5585b Ten0/9
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  channel-group 54 mode active

interface Ethernet1/3
  description ACE 2 Gig 1/1
  switchport mode trunk
  switchport trunk allowed vlan 149,912
  speed 1000
  channel-group 13
  vpc orphan-port suspend

interface Ethernet1/4
  description ACE 2 Gig 1/2
  switchport mode trunk
  switchport trunk allowed vlan 149,912
  speed 1000
  channel-group 13
  vpc orphan-port suspend

interface Ethernet1/5
  switchport mode fex-fabric
  fex associate 106
  channel-group 106
  no shutdown

interface Ethernet1/6
  switchport mode fex-fabric
  fex associate 106
  channel-group 106
  no shutdown

interface Ethernet1/7
  switchport mode fex-fabric
  fex associate 107
  channel-group 107
  no shutdown

interface Ethernet1/8
  switchport mode fex-fabric
  fex associate 107
  channel-group 107
  no shutdown
```

```
interface Ethernet1/9
  description Link to FI-A Eth 1/19
  switchport mode trunk
  switchport trunk allowed vlan 148-163
  channel-group 50 mode active
  no shutdown

interface Ethernet1/10
  description Link to FI-A Eth 1/20
  switchport mode trunk
  switchport trunk allowed vlan 148-163
  channel-group 50 mode active
  no shutdown

interface Ethernet1/11
  description Link to FI-B Eth 1/19
  switchport mode trunk
  switchport trunk allowed vlan 148-163
  channel-group 51 mode active
  no shutdown

interface Ethernet1/12
  description Link to FI-B Eth 1/20
  switchport mode trunk
  switchport trunk allowed vlan 148-163
  channel-group 51 mode active
  no shutdown

interface Ethernet1/13
  description Dual-Homed 2248TP FEX
  switchport mode fex-fabric
  fex associate 100
  channel-group 100
  no shutdown

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17
  description vPC Peer-Link
  switchport mode trunk
  channel-group 10 mode active
  no shutdown

interface Ethernet1/18
  description vPC Peer-Link
  switchport mode trunk
  channel-group 10 mode active
  no shutdown

interface Ethernet1/19
  description Link to Core-1
  no switchport
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  ip address 10.4.40.58/30
  ip router eigrp 100
  ip pim sparse-mode

interface Ethernet1/20
  description Link to Core-2
  no switchport
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  ip address 10.4.40.62/30
  ip router eigrp 100
  ip pim sparse-mode

interface Ethernet1/21
  description Link to Management Switch for VLAN 163
  switchport mode trunk
  switchport trunk allowed vlan 163
```

```
  speed 1000
  channel-group 21 mode active
  no shutdown

interface Ethernet1/22

interface Ethernet1/23
  description Dual-Homed 2232PP FEX
  switchport mode fex-fabric
  fex associate 103
  channel-group 103
  no shutdown

interface Ethernet1/24
  description Dual-Homed 2232PP FEX
  switchport mode fex-fabric
  fex associate 103
  channel-group 103
  no shutdown

interface Ethernet1/25
  description Dual-Homed 2232PP FEX
  switchport mode fex-fabric
  fex associate 104
  channel-group 104
  no shutdown

interface Ethernet1/26
  description Dual-Homed 2232PP FEX
  switchport mode fex-fabric
  fex associate 104
  channel-group 104
  no shutdown

interface Ethernet1/27
  description Link to EMC (VNX5700) SlotB2-P0
  switchport mode trunk
  switchport trunk allowed vlan 305
  spanning-tree port type edge trunk
  no shutdown

interface Ethernet1/28
  description Link to EMC (VNX5700) SlotA2-P1
  switchport mode trunk
  switchport trunk allowed vlan 305
  spanning-tree port type edge trunk
  no shutdown

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface Ethernet1/33

interface Ethernet1/34

interface Ethernet1/35

interface Ethernet1/36

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet1/41
```

```
interface Ethernet1/42

interface mgmt0
  ip address 10.4.63.11/24

interface loopback0
  ip address 10.4.56.253/32
  ip router eigrp 100
  ip pim sparse-mode

interface Ethernet103/1/1
  description Links to 7500-1 {Ten0/0/1}
  switchport mode trunk
  switchport trunk allowed vlan 146
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  no shutdown

interface Ethernet103/1/2
  description link to 7500-2
  switchport mode trunk
  switchport trunk allowed vlan 146
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  no shutdown

interface Ethernet103/1/3

!************************************************
! interfaces Ethernet103/1/4 to 103/1/31 are not
! configured and have been removed for brevity
!************************************************

interface Ethernet103/1/32

interface Ethernet104/1/1
  description link to 7500-2 (Ten0/0/1)
  switchport mode trunk
  switchport trunk allowed vlan 146
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  no shutdown

interface Ethernet104/1/2
  description link to 7500-2
  switchport mode trunk
  switchport trunk allowed vlan 146
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  no shutdown

interface Ethernet104/1/3

!************************************************
! interfaces Ethernet104/1/4 to 104/1/31 are not
! configured and have been removed for brevity
!************************************************

interface Ethernet104/1/32

interface Ethernet106/1/1
  description Link to WLC5508-1 (P1)
  switchport mode trunk
  switchport trunk allowed vlan 116,120,146
  channel-group 67
  no shutdown

interface Ethernet106/1/2
  description Link to WLC5508-1 (P2)
  switchport mode trunk
  switchport trunk allowed vlan 116,120,146
  channel-group 67
  no shutdown

interface Ethernet106/1/3
  switchport access vlan 148
  spanning-tree port type edge
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

```
  no shutdown

interface Ethernet106/1/4

!************************************************
! interfaces Ethernet106/1/5 to 106/1/45 are not
! configured and have been removed for brevity
!************************************************

interface Ethernet106/1/46

interface Ethernet106/1/47
  description LAB VPN Access
  switchport access vlan 148
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  no shutdown

interface Ethernet106/1/48
  description Connected to Backend ESX Server
  switchport mode trunk
  switchport trunk native vlan 148
  switchport trunk allowed vlan 148-163
  spanning-tree port type edge trunk
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  no shutdown

interface Ethernet107/1/1
  description Link to WLC5508-2 (P1)
  switchport mode trunk
  switchport trunk allowed vlan 116,120,146
  channel-group 68
  no shutdown

interface Ethernet107/1/2
  description Link to WLC5508-2 (P2)
  switchport mode trunk
  switchport trunk allowed vlan 116,120,146
  channel-group 68
  no shutdown

interface Ethernet107/1/3

interface Ethernet107/1/4

!************************************************
! interfaces Ethernet107/1/5 to 107/1/45 are not
! configured and have been removed for brevity
!************************************************

interface Ethernet107/1/46

interface Ethernet107/1/47
  description NTP Server
  switchport access vlan 148
  spanning-tree port type edge
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  no shutdown

interface Ethernet107/1/48
  description Openfiler
  switchport access vlan 148
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  no shutdown
clock timezone PST -8 0
clock summer-time PDT 2 Sunday march 02:00 1 Sunday nov 02:00 60
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.2.1.N1.1b.bin
boot system bootflash:/n5000-uk9.5.2.1.N1.1b.bin
router eigrp 100
  router-id 10.4.56.253
  redistribute static route-map static-to-eigrp
ip route 10.4.54.0/24 Vlan153 10.4.53.126
ip route 10.4.55.0/24 Vlan153 10.4.53.126
```

```
ip pim ssm range 232.0.0.0/8
ip pim auto-rp forward listen
no ip igmp snooping mrouter vpc-peer-link
system default switchport shutdown
vpc bind-vrf default vlan 900
interface fc1/45
interface fc1/46
interface fc1/47
interface fc1/48
interface fc1/43
interface fc1/44
interface fc1/45
interface fc1/46
interface fc1/47
  switchport mode E
interface fc1/48
  switchport mode E
zoneset distribute full vsan 5
!Full Zone Database Section for vsan 5
zone name p29-ucs-b-fc1-ch1s3_emc vsan 5
    member pwwn 50:06:01:61:47:20:2e:b7
!               [emc-a1-p1-fc]
    member pwwn 50:06:01:68:47:20:2e:b7
!               [emc-b1-p0-fc]
    member pwwn 20:ff:00:25:b5:0b:00:7f

zoneset name SAN_5 vsan 5
    member p29-ucs-b-fc1-ch1s3_emc

zoneset activate name SAN_5 vsan 5
```

Cisco MDS 9148a

The Cisco MDS 9100 Multilayer Fabric switches provide support for a higher density Fibre Channel SAN by extending Fibre Channel ports from the core Nexus 5500UP switches for larger environments. This Cisco MDS 9100 switch extends the Fibre Channel SAN-A network transport.

```
version 5.0(8)
feature tacacs+
role name default-role
  description This is a system defined role and applies to all
users.
  rule 5 permit show feature environment
  rule 4 permit show feature hardware
  rule 3 permit show feature module
  rule 2 permit show feature snmp
  rule 1 permit show feature system
username admin password 5 ***** role network-admin
ssh key rsa 2048
ip domain-lookup cisco.local
ip host MDS9148a 10.4.63.12
tacacs-server host 10.4.48.15 key 7 *****
aaa group server tacacs+ tacacs
    server 10.4.48.15
aaa group server radius radius
snmp-server user admin network-admin auth md5 ***** localizedkey
snmp-server host 10.4.48.30 traps version 2c public  udp-port
2162
rmon event 1 log trap public description FATAL(1) owner PMON@
FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@
CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@
ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@
WARNING
rmon event 5 log trap public description INFORMATION(5) owner
PMON@INFO
snmp-server community ***** group network-admin
```

```
snmp-server community ***** group network-operator
ntp server 10.4.48.17
aaa authentication login default group tacacs
vsan database
  vsan 4 name "General-Storage"
device-alias database
  device-alias name emc-a1-p0-fc pwwn 50:06:01:60:47:20:2e:b7
  device-alias name emc-b1-p1-fc pwwn 50:06:01:69:47:20:2e:b7

device-alias commit

fcdomain fcid database
  vsan 1 wwn 50:06:01:60:47:20:2e:b7 fcid 0xc70200 dynamic
!            [emc-a1-p0-fc]
  vsan 4 wwn 50:06:01:60:47:20:2e:b7 fcid 0x9c0000 dynamic
!            [emc-a1-p0-fc]
  vsan 1 wwn 25:00:00:05:73:b4:1e:80 fcid 0xc70000 dynamic
  vsan 1 wwn 20:41:00:05:73:a2:bd:40 fcid 0xc70100 dynamic
  vsan 1 wwn 50:06:01:69:47:20:2e:b7 fcid 0xc70300 dynamic
!            [emc-b1-p1-fc]
  vsan 4 wwn 50:06:01:69:47:20:2e:b7 fcid 0x9c0100 dynamic
!            [emc-b1-p1-fc]


interface port-channel 1
  switchport mode E
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 4
  switchport rate-mode dedicated
vsan database
  vsan 4 interface fc1/1
  vsan 4 interface fc1/2
clock timezone PST -8 0
clock summer-time PDT 2 Sunday march 02:00 1 Sunday nov 02:00 60
ip default-gateway 10.4.63.1
switchname MDS9148a
line console
boot kickstart bootflash:/m9100-s3ek9-kickstart-mz.5.0.8.bin
boot system bootflash:/m9100-s3ek9-mz.5.0.8.bin
interface fc1/13
  switchport rate-mode dedicated
interface fc1/14
  switchport rate-mode dedicated
interface fc1/1
interface fc1/2
interface fc1/3
interface fc1/4
interface fc1/5
interface fc1/6
interface fc1/7
interface fc1/8
interface fc1/9
interface fc1/10
interface fc1/11
interface fc1/12
interface fc1/15
interface fc1/16
interface fc1/17
interface fc1/18
interface fc1/19
interface fc1/20
interface fc1/21
interface fc1/22
interface fc1/23
interface fc1/24
interface fc1/25
interface fc1/26
interface fc1/27
interface fc1/28
interface fc1/29
interface fc1/30
interface fc1/31
interface fc1/32
interface fc1/33
```

```
interface fc1/34
interface fc1/35
interface fc1/36
interface fc1/37
interface fc1/38
interface fc1/39
interface fc1/40
interface fc1/41
interface fc1/42
interface fc1/43
interface fc1/44
interface fc1/45
interface fc1/46
interface fc1/47
interface fc1/48
interface fc1/13
  switchport mode E
interface fc1/14
  switchport mode E
system default zone distribute full
zoneset distribute full vsan 4
!Full Zone Database Section for vsan 4
zone name p29-ucs-b-fc0-ch1s3_emc vsan 4
    member pwwn 50:06:01:60:47:20:2e:b7
!               [emc-a1-p0-fc]
    member pwwn 50:06:01:69:47:20:2e:b7
!               [emc-b1-p1-fc]
    member pwwn 20:ff:00:25:b5:0a:00:7f

zone name p29-ucs-c220m3-2-fc0_emc vsan 4
    member pwwn 50:06:01:60:47:20:2e:b7
!               [emc-a1-p0-fc]
    member pwwn 50:06:01:69:47:20:2e:b7
!               [emc-b1-p1-fc]
    member pwwn 20:00:fc:99:47:24:f1:4f

zone name p29-ucs-c220m3-2-fc0_netapp-e1a vsan 4
    member pwwn 20:00:fc:99:47:24:f1:4f
    member pwwn 50:0a:09:81:8d:90:dc:42

zone name p29-ucs-c220m3-1-fc0_netapp-e1a vsan 4
    member pwwn 20:00:fc:99:47:25:23:6f
    member pwwn 50:0a:09:81:8d:90:dc:42

zone name VDI-Servers-SHARED-Storage-fc0_netapp-e1a vsan 4
    member pwwn 20:ff:00:25:b5:0a:00:5f
    member pwwn 50:0a:09:81:8d:90:dc:42

zone name p29-ucs-c220m3-2-vhba3_netapp-e1a vsan 4
    member pwwn 50:0a:09:81:8d:60:dc:42

zoneset name SAN_4 vsan 4
    member p29-ucs-b-fc0-ch1s3_emc
    member p29-ucs-c220m3-2-fc0_emc
    member p29-ucs-c220m3-2-fc0_netapp-e1a
    member p29-ucs-c220m3-1-fc0_netapp-e1a
    member VDI-Servers-SHARED-Storage-fc0_netapp-e1a

zoneset activate name SAN_4 vsan 4

interface fc1/1
  port-license acquire

interface fc1/2
  port-license acquire
  no shutdown

!************************************************
! Interfaces fc 1/3 to 1/11 are not
! configured and have been removed for brevity
!************************************************

interface fc1/12
  port-license acquire
```

```
interface fc1/13
  port-license acquire
  channel-group 1 force
  no shutdown

interface fc1/14
  port-license acquire
  channel-group 1 force
  no shutdown

interface fc1/15
  port-license acquire

!************************************************
! Interfaces fc 1/16 to 1/47 are not
! configured and have been removed for brevity
!************************************************

interface fc1/48

interface mgmt0
  ip address 10.4.63.12 255.255.255.0
no system default switchport shutdown
end
```

Cisco MDS 9148b

The Cisco MDS 9100 Multilayer Fabric switches provide support for a higher density Fibre Channel SAN by extending Fibre Channel ports from the core Nexus 5500UP switches for larger environments. This Cisco MDS 9100 switch extends the Fibre Channel SAN-B network transport.

```
version 5.0(8)
feature tacacs+
role name default-role
  description This is a system defined role and applies to all
users.
  rule 5 permit show feature environment
  rule 4 permit show feature hardware
  rule 3 permit show feature module
  rule 2 permit show feature snmp
  rule 1 permit show feature system
username admin password 5 ***** role network-admin
ssh key rsa 2048
ip domain-lookup
ip host MDS9148b 10.4.63.13
tacacs-server host 10.4.48.15 key 7 *****
aaa group server tacacs+ tacacs
    server 10.4.48.15
aaa group server radius radius
snmp-server user admin network-admin auth md5 ***** localizedkey
snmp-server host 10.4.48.30 traps version 2c public  udp-port
2162
rmon event 1 log trap public description FATAL(1) owner PMON@
FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@
CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@
ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@
WARNING
rmon event 5 log trap public description INFORMATION(5) owner
PMON@INFO
snmp-server community ***** group network-operator
snmp-server community ***** group network-admin
ntp server 10.4.48.17
aaa authentication login default group tacacs
vsan database
  vsan 5 name "General-Storage"
device-alias database
  device-alias name emc-a1-p1-fc pwwn 50:06:01:61:47:20:2e:b7
  device-alias name emc-b1-p0-fc pwwn 50:06:01:68:47:20:2e:b7

device-alias commit
```

```
fcdomain fcid database
  vsan 1 wwn 20:41:00:05:73:f1:b2:00 fcid 0x1f0000 dynamic
  vsan 1 wwn 20:42:00:05:73:f1:b2:00 fcid 0x1f0100 dynamic
  vsan 1 wwn 50:06:01:68:47:20:2e:b7 fcid 0x1f0200 dynamic
!            [emc-b1-p0-fc]
  vsan 5 wwn 50:06:01:68:47:20:2e:b7 fcid 0xa30000 dynamic
!            [emc-b1-p0-fc]
  vsan 1 wwn 50:06:01:61:47:20:2e:b7 fcid 0x1f0300 dynamic
!            [emc-a1-p1-fc]
  vsan 5 wwn 50:06:01:61:47:20:2e:b7 fcid 0xa30100 dynamic
!            [emc-a1-p1-fc]


interface port-channel 1
  switchport mode E
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 5
  switchport rate-mode dedicated
vsan database
  vsan 5 interface fc1/1
  vsan 5 interface fc1/2
clock timezone PST -8 0
clock summer-time PDT 2 Sunday march 02:00 1 Sunday nov 02:00 60
ip default-gateway 10.4.63.1
switchname MDS9148b
line console
boot kickstart bootflash:/m9100-s3ek9-kickstart-mz.5.0.8.bin
boot system bootflash:/m9100-s3ek9-mz.5.0.8.bin
interface fc1/13
  switchport rate-mode dedicated
interface fc1/14
  switchport rate-mode dedicated
interface fc1/1
interface fc1/2
interface fc1/3
interface fc1/4
interface fc1/5
interface fc1/6
interface fc1/7
interface fc1/8
interface fc1/9
interface fc1/10
interface fc1/11
interface fc1/12
interface fc1/15
interface fc1/16
interface fc1/17
interface fc1/18
interface fc1/19
interface fc1/20
interface fc1/21
interface fc1/22
interface fc1/23
interface fc1/24
interface fc1/25
interface fc1/26
interface fc1/27
interface fc1/28
interface fc1/29
interface fc1/30
interface fc1/31
interface fc1/32
interface fc1/33
interface fc1/34
interface fc1/35
interface fc1/36
interface fc1/37
interface fc1/38
interface fc1/39
interface fc1/40
interface fc1/41
interface fc1/42
interface fc1/43
interface fc1/44
```

```
interface fc1/45
interface fc1/46
interface fc1/47
interface fc1/48
interface fc1/13
  switchport mode E
interface fc1/14
  switchport mode E
system default zone distribute full
zoneset distribute full vsan 5
!Full Zone Database Section for vsan 5
zone name p29-ucs-b-fc1-ch1s3_emc vsan 5
    member pwwn 50:06:01:61:47:20:2e:b7
!               [emc-a1-p1-fc]
    member pwwn 50:06:01:68:47:20:2e:b7
!               [emc-b1-p0-fc]
    member pwwn 20:ff:00:25:b5:0b:00:7f

zone name p29-ucs-c220m3-2-fc1_netapp-e1b vsan 5
    member pwwn 20:00:fc:99:47:24:f1:50
    member pwwn 50:06:01:61:47:20:2e:b7
!               [emc-a1-p1-fc]
    member pwwn 50:06:01:68:47:20:2e:b7
!               [emc-b1-p0-fc]

zone name VDI-Servers-SHARED-Storage-fc1_netapp-e1b vsan 5
    member pwwn 20:ff:00:25:b5:0b:00:5f
    member pwwn 50:0a:09:82:8d:90:dc:42

zoneset name SAN_5 vsan 5
    member p29-ucs-b-fc1-ch1s3_emc
    member p29-ucs-c220m3-2-fc1_netapp-e1b
    member VDI-Servers-SHARED-Storage-fc1_netapp-e1b

zoneset activate name SAN_5 vsan 5

interface fc1/1
  port-license acquire
interface fc1/2
  port-license acquire
  no shutdown

!************************************************
! Interfaces fc 1/3 to 1/11 are not
! configured and have been removed for brevity
!************************************************

interface fc1/12
  port-license acquire

interface fc1/13
  port-license acquire
  channel-group 1 force
  no shutdown

interface fc1/14
  port-license acquire
  channel-group 1 force
  no shutdown

interface fc1/15
  port-license acquire

!************************************************
! Interfaces fc 1/16 to 1/47 are not
! configured and have been removed for brevity
!************************************************

interface fc1/48

interface mgmt0
  ip address 10.4.63.13 255.255.255.0
no system default switchport shutdown
end
```

Cisco Catalyst 2960s Management Switch

The Cisco Catalyst 2960-S provides the Ethernet out-of-band network for the data center switches, servers, and appliances. The Cisco Catalyst 3750X and 3560X series switches can be used to provide a more resilient Ethernet out-of-band network transport.

```
version 15.0
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname DC-Mgmt2960S
!
boot-start-marker
boot-end-marker
!
enable secret 4 *****
!
username admin password 7 *****
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
switch 1 provision ws-c2960s-48fpd-l
authentication mac-move permit
!
ip name-server 10.4.48.10
vtp mode transparent
udld enable
!
mls qos map policed-dscp  0 10 18 24 46 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41
42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19
20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29
30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51
52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59
60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13
15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!
crypto pki trustpoint TP-self-signed-3972451072
 enrollment selfsigned
```

```
 subject-name cn=IOS-Self-Signed-Certificate-3972451072
 revocation-check none
 rsakeypair TP-self-signed-3972451072
!
!
crypto pki certificate chain TP-self-signed-3972451072
 certificate self-signed 02
  3082022B 30820194 A0030201 …
       quit
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
port-channel load-balance src-dst-ip
!
vlan internal allocation policy ascending
!
vlan 163
 name DC_ManagementVLAN
!
macro name EgressQoS
mls qos trust dscp
queue-set 1
srr-queue bandwidth share 1 30 35 5
priority-queue out
@

!
interface Port-channel1
 description Etherchannel Link to DC Core for Layer 3
 switchport trunk allowed vlan 163
 switchport mode trunk
 logging event link-status
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet1/0/1
 switchport access vlan 163
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 description Link to MDS9148 mgmt0
 switchport access vlan 163
 switchport mode access
 duplex full
 spanning-tree portfast
!
interface GigabitEthernet1/0/3
 description Link to MDS9148 mgmt0
 switchport access vlan 163
 switchport mode access
 duplex full
 spanning-tree portfast
!
interface GigabitEthernet1/0/4
 description Link to N5K-C5596 mgmt0
 switchport access vlan 163
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/5
 description Link to N5K-C5596 mgmt0
 switchport access vlan 163
 switchport mode access
 spanning-tree portfast
!
!************************************************
! Interfaces GigabitEthernet 1/0/6 to 1/0/46 are
! configured the same way and have been removed for brevity
!************************************************
```

```
!
interface GigabitEthernet1/0/47
 description Link to DC5596a {Ethernet 1/21}
 switchport trunk allowed vlan 163
 switchport mode trunk
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 channel-group 1 mode active
!
interface GigabitEthernet1/0/48
 description Link to DC5596b {Ethernet 1/21}
 switchport trunk allowed vlan 163
 switchport mode trunk
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 channel-group 1 mode active
!
interface GigabitEthernet1/0/49
!
interface GigabitEthernet1/0/50
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan163
 description in-band management
 ip address 10.4.63.5 255.255.255.0
!
ip default-gateway 10.4.63.1
no ip http server
ip http authentication aaa
ip http secure-server
!
ip sla enable reaction-alerts
logging 10.4.48.35
logging 10.4.48.38
logging 10.4.48.39
snmp-server community ***** RO
snmp-server community ***** RW
snmp-server host 10.4.48.35 *****
snmp-server host 10.4.48.38 *****
snmp-server host 10.4.48.35 *****
snmp-server host 10.4.48.39 *****
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 *****
!
line con 0
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
ntp server 10.4.48.17
end
```

Cisco ASA 5585—Primary

The Cisco ASA 5585 firewalls for the Cisco SBA data center are provisioned in pairs for resiliency. This is the primary firewall configuration.

```
ASA Version 9.0(1)
!
hostname DC-ASA5585X
domain-name cisco.local
enable password ***** encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/1
 description LAN/STATE Failover Interface
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
!************************************************
! Interfaces GigabitEthernet 0/3 to 0/6 are
! unconfigured and have been removed for brevity
!************************************************
!
interface GigabitEthernet0/7
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface TenGigabitEthernet0/8
 description Trunk to DC5548x eth1/1
 channel-group 10 mode passive
 no nameif
 no security-level
 no ip address
```

```
!
interface TenGigabitEthernet0/9
 description Trunk to DC5548x eth1/2
 channel-group 10 mode passive
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/0
 shutdown
 no nameif
 no security-level
 no ip address
!
!************************************************
! Interfaces GigabitEthernet 1/1 to 1/7
! are unconfigured and have been removed for brevity
!************************************************
!
interface TenGigabitEthernet1/8
 shutdown
 no nameif
 no security-level
 no ip address
!
interface TenGigabitEthernet1/9
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Port-channel10
 description ECLB Trunk to 5548 Switches
 no nameif
 no security-level
 no ip address
!
interface Port-channel10.153
 description DC VLAN Outside the FW
 vlan 153
 nameif outside
 security-level 0
 ip address 10.4.53.126 255.255.255.128 standby 10.4.53.125
!
interface Port-channel10.154
 description DC VLAN Inside the Firewall
 vlan 154
 nameif DC-InsideFW
 security-level 75
 ip address 10.4.54.1 255.255.255.0 standby 10.4.54.2
!
interface Port-channel10.155
 description DC VLAN Inside the FW w/ IPS
 vlan 155
 nameif DC-InsideIPS
 security-level 75
 ip address 10.4.55.1 255.255.255.0 standby 10.4.55.2
!
interface Port-channel10.157
 description DC VDI_Desktop VLAN
 vlan 157
 nameif DC-VDI_Desktop
 security-level 75
 ip address 10.4.57.1 255.255.255.0 standby 10.4.57.2
!
boot system disk0:/asa901-smp-k8.bin
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns server-group DefaultDNS
 domain-name cisco.local
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network IT_Web_Server
```

```
 host 10.4.54.80
object network HR_Web_Server
 host 10.4.55.80
object network Finance_Web_Server
 host 10.4.54.81
object network Research_Web_Server
 host 10.4.55.81
object service Citrix2593
 service tcp destination eq 2598
 description Citrix ICA Port 2593
object service Citrix1494
 service tcp destination eq citrix-ica
 description Citrix ICA Port 1494
object service Citrix1604
 service tcp destination eq 1604
 description Citrix ICA Port 1604
object service RDP
 service tcp destination eq 3389
 description RDP
object network Dan-Host
 host 10.4.55.67
object network Secure_Subnets
 subnet 10.4.54.0 255.255.255.0
object-group service DM_INLINE_SERVICE_2
 service-object tcp destination eq ssh
 service-object udp destination eq snmp
object-group service DM_INLINE_TCP_2 tcp
 port-object eq www
 port-object eq https
object-group service DM_INLINE_TCP_3 tcp
 port-object eq www
 port-object eq https
object-group service DM_INLINE_TCP_4 tcp
 port-object eq www
 port-object eq https
object-group service DM_INLINE_SERVICE_1
 service-object icmp
 service-object udp destination eq bootpc
 service-object udp destination eq bootps
 service-object udp destination eq domain
 service-object tcp destination eq www
 service-object tcp destination eq https
object-group network DM_INLINE_NETWORK_1
 network-object object Finance_Web_Server
 network-object object HR_Web_Server
 network-object object IT_Web_Server
 network-object object Research_Web_Server
object-group service DM_INLINE_TCP_5 tcp
 port-object eq www
 port-object eq https
object-group service DM_INLINE_TCP_6 tcp
 port-object eq www
 port-object eq https
object-group network DM_INLINE_NETWORK_2
 network-object object Finance_Web_Server
 network-object object HR_Web_Server
 network-object object IT_Web_Server
 network-object object Research_Web_Server
object-group protocol DM_INLINE_PROTOCOL_1
 protocol-object ip
 protocol-object icmp
object-group service DM_INLINE_SERVICE_3
 service-object object Citrix1494
 service-object object Citrix1604
 service-object object Citrix2593
 service-object object RDP
object-group service DM_INLINE_SERVICE_4
 service-object icmp
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 service-object ip
access-list DC-InsideIPS_mpc extended permit ip any4 any4
access-list global_access extended permit object-group DM_INLINE_
```

```
SERVICE_1 any4 object-group DM_INLINE_NETWORK_2
access-list global_access extended permit tcp security-group name
IT_Users any4 object IT_Web_Server object-group DM_INLINE_TCP_6
log
access-list global_access remark Permit HTTP(S) to Web server 2
access-list global_access extended permit tcp security-group name
Finance_Users any4 object Finance_Web_Server object-group DM_
INLINE_TCP_3
access-list global_access remark Permit HTTP(S) to Web server 3
access-list global_access extended permit tcp security-group name
HR_Users any4 object HR_Web_Server object-group DM_INLINE_TCP_2
access-list global_access remark Permit HTTP(S) to Web server 4
access-list global_access extended permit tcp security-group name
Research_Users any4 object Research_Web_Server object-group DM_
INLINE_TCP_4
access-list global_access extended permit tcp object-group DM_
INLINE_NETWORK_1 any4 object-group DM_INLINE_TCP_5
access-list global_access extended permit ip any 10.4.57.0
255.255.255.0 log inactive
access-list global_access extended permit object-group DM_INLINE_
SERVICE_2 10.4.53.0 255.255.255.128 object Secure_Subnets
access-list global_access remark VDI desktop access
access-list global_access extended permit object-group DM_INLINE_
PROTOCOL_1 10.4.57.0 255.255.255.0 any4
access-list global_access remark Management access to VDI
solution
access-list global_access extended permit object-group DM_INLINE_
SERVICE_4 any4 10.4.57.0 255.255.255.0
access-list global_access remark Citrix Receiver clients to VDI
access-list global_access extended permit object-group DM_INLINE_
SERVICE_3 any4 10.4.57.0 255.255.255.0
access-list DC-InsideIPS_mpc_1 extended permit ip any4 any4
pager lines 24
logging enable
logging asdm informational
mtu outside 1500
mtu DC-InsideFW 1500
mtu DC-InsideIPS 1500
mtu DC-VDI_Desktop 1500
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/1
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key *****
failover replication http
failover link failover GigabitEthernet0/1
failover interface ip failover 10.4.53.130 255.255.255.252
standby 10.4.53.129
monitor-interface outside
monitor-interface DC-InsideFW
monitor-interface DC-InsideIPS
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-702.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group global_access global
route outside 0.0.0.0 0.0.0.0 10.4.53.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (outside) host 10.4.48.15
 key *****
aaa-server ISE-Group protocol radius
```

```
aaa-server ISE-Group (outside) host 10.4.48.41
 key *****
cts server-group ISE-Group
cts sxp enable
cts sxp default password *****
cts sxp default source-ip 10.4.53.126
cts sxp connection peer 10.4.15.254 password default mode local
listener
cts sxp connection peer 10.4.32.241 password default mode local
listener
cts sxp connection peer 10.4.32.242 password default mode local
listener
cts sxp connection peer 10.4.63.28 password default mode local
listener
user-identity default-domain LOCAL
aaa authentication enable console AAA-SERVER LOCAL
aaa authentication ssh console AAA-SERVER LOCAL
aaa authentication http console AAA-SERVER LOCAL
aaa authentication serial console AAA-SERVER LOCAL
aaa authorization exec authentication-server
http server enable
http 10.4.48.0 255.255.255.0 outside
snmp-server host outside 10.4.48.35 community *****
no snmp-server location
no snmp-server contact
snmp-server community *****
snmp-server enable traps snmp authentication linkup linkdown
coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh 10.4.48.0 255.255.255.0 outside
ssh timeout 5
ssh version 2
console timeout 0
dhcprelay server 10.4.48.10 outside
dhcprelay enable DC-VDI_Desktop
dhcprelay setroute DC-VDI_Desktop
dhcprelay timeout 60
!
tls-proxy maximum-session 1000
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 10.4.48.17
ssl encryption aes256-sha1 aes128-sha1 3des-sha1
username admin password ***** encrypted
!
class-map DC-InsideIPS-class
 match access-list DC-InsideIPS_mpc_1
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
```

```
  inspect sip
  inspect xdmcp
policy-map DC-InsideIPS-policy
 class DC-InsideIPS-class
  ips inline fail-close
!
service-policy global_policy global
service-policy DC-InsideIPS-policy interface DC-InsideIPS
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/
oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly 11
  subscribe-to-alert-group configuration periodic monthly 11
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:47500a204037fd77e73ec06aca3e56c8
: end
```

Cisco ASA 5585 IPS SSP—Primary

The Cisco ASA 5585 firewall for the Cisco SBA data center is provisioned with an internal Intrusion Prevention System (IPS) security services processor (SSP). The combined Cisco ASA firewall and IPS operate in resilient pairs. This is the primary Cisco ASA 5585 IPS SSP.

```
! Version 7.1(6)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S648.0   2012-05-30
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Enabled
risk-rating-range 100-100
exit
exit
! ------------------------------
service host
network-settings
host-ip 10.4.63.21/24,10.4.63.1
host-name IPS-SSP20-A
telnet-option disabled
access-list 10.4.48.0/24
dns-primary-server enabled
address 10.4.48.10
exit
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset -480
standard-time-zone-name GMT-08:00
exit
ntp-option enabled-ntp-unauthenticated
ntp-server 10.4.48.17
exit
summertime-option recurring
summertime-zone-name UTC
exit
exit
! ------------------------------
service logger
```

```
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
network-participation partial
exit
! ------------------------------
service aaa
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
physical-interface PortChannel0/0
exit
```

Cisco ASA 5585—Secondary

The Cisco ASA 5585 Adaptive Security Appliances for the Cisco SBA data center are provisioned in pairs for resiliency. Although this is the secondary Cisco ASA 5585, the configuration is the same as the primary Cisco ASA 5585, with the exception of a few lines.

```
ASA Version 9.0(1)
!
hostname DC-ASA5585X
domain-name cisco.local
enable password ***** encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/1
 description LAN/STATE Failover Interface
!
interface GigabitEthernet0/2
 shutdown
 no nameif
```

```
 no security-level
 no ip address
!
!*************************************************
! Interfaces GigabitEthernet 0/3 to 0/6 are
! unconfigured and have been removed for brevity
!*************************************************
!
interface GigabitEthernet0/7
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface TenGigabitEthernet0/8
 description Trunk to DC5548x eth1/1
 channel-group 10 mode passive
 no nameif
 no security-level
 no ip address
!
interface TenGigabitEthernet0/9
 description Trunk to DC5548x eth1/2
 channel-group 10 mode passive
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/0
 shutdown
 no nameif
 no security-level
 no ip address
!
!*************************************************
! Interfaces GigabitEthernet 1/1 to 1/7
! are unconfigured and have been removed for brevity
!*************************************************
!
interface TenGigabitEthernet1/8
 shutdown
 no nameif
 no security-level
 no ip address
!
interface TenGigabitEthernet1/9
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Port-channel10
 description ECLB Trunk to 5548 Switches
 no nameif
 no security-level
 no ip address
!
interface Port-channel10.153
 description DC VLAN Outside the FW
 vlan 153
 nameif outside
 security-level 0
```

```
 ip address 10.4.53.126 255.255.255.128 standby 10.4.53.125
!
interface Port-channel10.154
 description DC VLAN Inside the Firewall
 vlan 154
 nameif DC-InsideFW
 security-level 75
 ip address 10.4.54.1 255.255.255.0 standby 10.4.54.2
!
interface Port-channel10.155
 description DC VLAN Inside the FW w/ IPS
 vlan 155
 nameif DC-InsideIPS
 security-level 75
 ip address 10.4.55.1 255.255.255.0 standby 10.4.55.2
!
interface Port-channel10.157
 description DC VDI_Desktop VLAN
 vlan 157
 nameif DC-VDI_Desktop
 security-level 75
 ip address 10.4.57.1 255.255.255.0 standby 10.4.57.2
!
boot system disk0:/asa901-smp-k8.bin
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns server-group DefaultDNS
 domain-name cisco.local
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network IT_Web_Server
 host 10.4.54.80
object network HR_Web_Server
 host 10.4.55.80
object network Finance_Web_Server
 host 10.4.54.81
object network Research_Web_Server
 host 10.4.55.81
object service Citrix2593
 service tcp destination eq 2598
 description Citrix ICA Port 2593
object service Citrix1494
 service tcp destination eq citrix-ica
 description Citrix ICA Port 1494
object service Citrix1604
 service tcp destination eq 1604
 description Citrix ICA Port 1604
object service RDP
 service tcp destination eq 3389
 description RDP
object network Dan-Host
 host 10.4.55.67
object network Secure_Subnets
 subnet 10.4.54.0 255.255.255.0
object-group service DM_INLINE_SERVICE_2
 service-object tcp destination eq ssh
 service-object udp destination eq snmp
object-group service DM_INLINE_TCP_2 tcp
 port-object eq www
 port-object eq https
object-group service DM_INLINE_TCP_3 tcp
 port-object eq www
 port-object eq https
object-group service DM_INLINE_TCP_4 tcp
 port-object eq www
 port-object eq https
object-group service DM_INLINE_SERVICE_1
 service-object icmp
 service-object udp destination eq bootpc
 service-object udp destination eq bootps
 service-object udp destination eq domain
 service-object tcp destination eq www
 service-object tcp destination eq https
```

```
object-group network DM_INLINE_NETWORK_1
 network-object object Finance_Web_Server
 network-object object HR_Web_Server
 network-object object IT_Web_Server
 network-object object Research_Web_Server
object-group service DM_INLINE_TCP_5 tcp
 port-object eq www
 port-object eq https
object-group service DM_INLINE_TCP_6 tcp
 port-object eq www
 port-object eq https
object-group network DM_INLINE_NETWORK_2
 network-object object Finance_Web_Server
 network-object object HR_Web_Server
 network-object object IT_Web_Server
 network-object object Research_Web_Server
object-group protocol DM_INLINE_PROTOCOL_1
 protocol-object ip
 protocol-object icmp
object-group service DM_INLINE_SERVICE_3
 service-object object Citrix1494
 service-object object Citrix1604
 service-object object Citrix2593
 service-object object RDP
object-group service DM_INLINE_SERVICE_4
 service-object icmp
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 service-object ip
access-list DC-InsideIPS_mpc extended permit ip any4 any4
access-list global_access extended permit object-group DM_INLINE_
SERVICE_1 any4 object-group DM_INLINE_NETWORK_2
access-list global_access extended permit tcp security-group name
IT_Users any4 object IT_Web_Server object-group DM_INLINE_TCP_6
log
access-list global_access remark Permit HTTP(S) to Web server 2
access-list global_access extended permit tcp security-group name
Finance_Users any4 object Finance_Web_Server object-group DM_
INLINE_TCP_3
access-list global_access remark Permit HTTP(S) to Web server 3
access-list global_access extended permit tcp security-group name
HR_Users any4 object HR_Web_Server object-group DM_INLINE_TCP_2
access-list global_access remark Permit HTTP(S) to Web server 4
access-list global_access extended permit tcp security-group name
Research_Users any4 object Research_Web_Server object-group DM_
INLINE_TCP_4
access-list global_access extended permit tcp object-group DM_
INLINE_NETWORK_1 any4 object-group DM_INLINE_TCP_5
access-list global_access extended permit ip any 10.4.57.0
255.255.255.0 log inactive
access-list global_access extended permit object-group DM_INLINE_
SERVICE_2 10.4.53.0 255.255.255.128 object Secure_Subnets
access-list global_access remark VDI desktop access
access-list global_access extended permit object-group DM_INLINE_
PROTOCOL_1 10.4.57.0 255.255.255.0 any4
access-list global_access remark Management access to VDI
solution
access-list global_access extended permit object-group DM_INLINE_
SERVICE_4 any4 10.4.57.0 255.255.255.0
access-list global_access remark Citrix Receiver clients to VDI
access-list global_access extended permit object-group DM_INLINE_
SERVICE_3 any4 10.4.57.0 255.255.255.0
access-list DC-InsideIPS_mpc_1 extended permit ip any4 any4
access-list DC-InsideIPS_mpc_2 extended permit ip any4 any4
pager lines 24
logging enable
logging asdm informational
mtu outside 1500
mtu DC-InsideFW 1500
mtu DC-InsideIPS 1500
mtu DC-VDI_Desktop 1500
failover
failover lan unit secondary
```

```
failover lan interface failover GigabitEthernet0/1
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key *****
failover replication http
failover link failover GigabitEthernet0/1
failover interface ip failover 10.4.53.130 255.255.255.252
standby 10.4.53.129
monitor-interface outside
monitor-interface DC-InsideFW
monitor-interface DC-InsideIPS
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-702.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group global_access global
route outside 0.0.0.0 0.0.0.0 10.4.53.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (outside) host 10.4.48.15
 key *****
aaa-server ISE-Group protocol radius
aaa-server ISE-Group (outside) host 10.4.48.41
 key *****
cts server-group ISE-Group
cts sxp enable
cts sxp default password *****
cts sxp default source-ip 10.4.53.126
cts sxp connection peer 10.4.15.254 password default mode local
listener
cts sxp connection peer 10.4.32.241 password default mode local
listener
cts sxp connection peer 10.4.32.242 password default mode local
listener
cts sxp connection peer 10.4.63.28 password default mode local
listener
user-identity default-domain LOCAL
aaa authentication enable console AAA-SERVER LOCAL
aaa authentication ssh console AAA-SERVER LOCAL
aaa authentication http console AAA-SERVER LOCAL
aaa authentication serial console AAA-SERVER LOCAL
aaa authorization exec authentication-server
http server enable
http 10.4.48.0 255.255.255.0 outside
snmp-server host outside 10.4.48.35 community *****
no snmp-server location
no snmp-server contact
snmp-server community *****
snmp-server enable traps snmp authentication linkup linkdown
coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh 10.4.48.0 255.255.255.0 outside
ssh timeout 5
ssh version 2
console timeout 0
dhcprelay server 10.4.48.10 outside
dhcprelay enable DC-VDI_Desktop
dhcprelay setroute DC-VDI_Desktop
dhcprelay timeout 60
!
tls-proxy maximum-session 1000
```

```
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 10.4.48.17
ssl encryption aes256-sha1 aes128-sha1 3des-sha1
username admin password w2Y.6Op4j7clVDk2 encrypted
!
class-map DC-InsideIPS-class
 match access-list DC-InsideIPS_mpc_2
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
policy-map DC-InsideIPS-policy
 class DC-InsideIPS-class
  ips inline fail-close
!
service-policy global_policy global
service-policy DC-InsideIPS-policy interface DC-InsideIPS
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/
oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly 11
  subscribe-to-alert-group configuration periodic monthly 11
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:bca0b4996edcca8d71d24471967e3ada
: end
```

Cisco ASA 5585 IPS SSP—Secondary

The Cisco ASA 5585 Adaptive Security Appliance for the Cisco SBA data center is provisioned with an internal IPS SSP. The combined Cisco ASA and IPS operate in resilient pairs. Although this is the secondary Cisco ASA IPS SSP in the secondary Cisco ASA, the configuration is the same as the primary Cisco ASA IPS SSP in the primary Cisco ASA, with the exception of a few lines.

```
! Version 7.1(6)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S648.0   2012-05-30
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
```

```
! ------------------------------
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Enabled
risk-rating-range 100-100
exit
exit
! ------------------------------
service host
network-settings
host-ip 10.4.63.23/24,10.4.63.1
host-name IPS-SSP20-B
telnet-option disabled
access-list 10.4.48.0/24
dns-primary-server enabled
address 10.4.48.10
exit
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset -480
standard-time-zone-name GMT-08:00
exit
ntp-option enabled-ntp-unauthenticated
ntp-server 10.4.48.17
exit
summertime-option recurring
summertime-zone-name UTC
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
network-participation partial
exit
! ------------------------------
service aaa
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
physical-interface PortChannel0/0
exit
exit
```

Cisco ACE—Primary

This Cisco ACE 4710 appliance is one of a resilient pair providing Layer 4 through Layer 7 switching services for the Cisco SBA data center. This is the primary ACE in the pair.

```
no ft auto-sync startup-config
logging enable
logging timestamp
logging trap 5
logging host 10.4.48.35 udp/514 format emblem
boot system image:c4710ace-t1k9-mz.A5_1_2.bin
peer hostname ACE4710-B
hostname ACE4710-A
interface gigabitEthernet 1/1
  channel-group 1
  no shutdown
interface gigabitEthernet 1/2
  channel-group 1
  no shutdown
interface gigabitEthernet 1/3
  shutdown
interface gigabitEthernet 1/4
  shutdown
interface port-channel 1
  ft-port vlan 912
  switchport trunk native vlan 1
  switchport trunk allowed vlan 149
  no shutdown
ntp server 10.4.48.17
access-list ALL line 8 extended permit ip any any

probe http http-probe
  request method head
  expect status 200 200
probe icmp icmp-probe
rserver redirect redirect1
  conn-limit max 4000000 min 4000000
  webhost-redirection https://%h%p 302
  inservice
rserver host webserver1
  ip address 10.4.49.111
  conn-limit max 4000000 min 4000000
  probe icmp-probe
  inservice
rserver host webserver2
  ip address 10.4.49.112
  conn-limit max 4000000 min 4000000
  probe icmp-probe
  inservice
rserver host webserver3
  ip address 10.4.49.113
  conn-limit max 4000000 min 4000000
  probe icmp-probe
  inservice
rserver host webserver4
  ip address 10.4.49.114
  conn-limit max 4000000 min 4000000
  probe icmp-probe
  inservice

serverfarm host appfarm
  probe http-probe
  rserver webserver3 80
    conn-limit max 4000000 min 4000000
```

```
    inservice
  rserver webserver4 80
    conn-limit max 4000000 min 4000000
    inservice
serverfarm redirect http-redirect
  rserver redirect1
    conn-limit max 4000000 min 4000000
    inservice
serverfarm host webfarm
  probe http-probe
  inband-health check log 5 reset 500
  retcode 404 404 check log 5 reset 10
  retcode 500 505 check log 5 reset 10
  rserver webserver1 80
    conn-limit max 4000000 min 4000000
    inservice
  rserver webserver2 80
    conn-limit max 4000000 min 4000000
    inservice

sticky http-cookie APPSESSIONID app-sticky
  cookie insert browser-expire
  serverfarm appfarm

ssl-proxy service app-ssl-proxy
  key cisco-sample-key
  cert cisco-sample-cert

class-map type http loadbalance match-any default-compression-
exclusion-mime-type
  description DM generated classmap for default LB compression
exclusion mime types.
  2 match http url .*gif
  3 match http url .*css
  4 match http url .*js
  5 match http url .*class
  6 match http url .*jar
  7 match http url .*cab
  8 match http url .*txt
  9 match http url .*ps
  10 match http url .*vbs
  11 match http url .*xsl
  12 match http url .*xml
  13 match http url .*pdf
  14 match http url .*swf
  15 match http url .*jpg
  16 match http url .*jpeg
  17 match http url .*jpe
  18 match http url .*png
class-map match-all http-vip
  2 match virtual-address 10.4.49.100 tcp eq www
class-map match-all http-vip-redirect
  2 match virtual-address 10.4.49.101 tcp eq www
class-map match-all https-vip
  2 match virtual-address 10.4.49.101 tcp eq https
class-map type management match-any remote_access
  2 match protocol xml-https any
  3 match protocol icmp any
  4 match protocol telnet any
  5 match protocol ssh any
  6 match protocol http any
  7 match protocol https any
  8 match protocol snmp any

policy-map type management first-match remote_mgmt_allow_policy
  class remote_access
    permit

policy-map type loadbalance first-match http-vip-l7slb
  class default-compression-exclusion-mime-type
    serverfarm webfarm
  class class-default
    serverfarm webfarm
    compress default-method deflate
```

```
policy-map type loadbalance first-match http-vip-redirect-l7slb
  class class-default
    serverfarm http-redirect
policy-map type loadbalance first-match https-vip-l7slb
  class default-compression-exclusion-mime-type
    sticky-serverfarm app-sticky
  class class-default
    compress default-method deflate
    sticky-serverfarm app-sticky

policy-map multi-match int149
  class https-vip
    loadbalance vip inservice
    loadbalance policy https-vip-l7slb
    nat dynamic 1 vlan 149
    ssl-proxy server app-ssl-proxy
  class http-vip-redirect
    loadbalance vip inservice
    loadbalance policy http-vip-redirect-l7slb
  class http-vip
    loadbalance vip inservice
    loadbalance policy http-vip-l7slb
    nat dynamic 1 vlan 149

interface vlan 149
  ip address 10.4.49.119 255.255.255.0
  peer ip address 10.4.49.120 255.255.255.0
  access-group input ALL
  nat-pool 1 10.4.49.99 10.4.49.99 netmask 255.255.255.0 pat
  service-policy input remote_mgmt_allow_policy
  service-policy input int149
  no shutdown

ft interface vlan 912
  ip address 10.255.255.1 255.255.255.0
  peer ip address 10.255.255.2 255.255.255.0
  no shutdown

ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 912
ft group 1
  peer 1
  associate-context Admin
  inservice

ip route 0.0.0.0 0.0.0.0 10.4.49.1

snmp-server community ***** group Network-Monitor


username admin password 5 ***** role Admin domain default-domain
username www password 5 ***** role Admin domain default-domain
```

Cisco ACE—Secondary

This Cisco ACE 4710 is one of a resilient pair providing Layer 4 through Layer 7 switching services for the Cisco SBA data center. Although this is the secondary Cisco ACE in the pair, the configuration is the same as the primary Cisco ACE, with the exception of a few lines.

```
no ft auto-sync startup-config
logging enable
logging timestamp
logging trap 5
logging host 10.4.48.35 udp/514 format emblem
boot system image:c4710ace-t1k9-mz.A5_1_2.bin
peer hostname ACE4710-A
hostname ACE4710-B
interface gigabitEthernet 1/1
  channel-group 1
  no shutdown
interface gigabitEthernet 1/2
  channel-group 1
  no shutdown
```

```
interface gigabitEthernet 1/3
  shutdown
interface gigabitEthernet 1/4
  shutdown
interface port-channel 1
  ft-port vlan 912
  switchport trunk native vlan 1
  switchport trunk allowed vlan 149
  no shutdown
ntp server 10.4.48.17
access-list ALL line 8 extended permit ip any any

probe http http-probe
  request method head
  expect status 200 200
probe icmp icmp-probe

rserver redirect redirect1
  conn-limit max 4000000 min 4000000
  webhost-redirection https://%h%p 302
  inservice
rserver host webserver1
  ip address 10.4.49.111
  conn-limit max 4000000 min 4000000
  probe icmp-probe
  inservice
rserver host webserver2
  ip address 10.4.49.112
  conn-limit max 4000000 min 4000000
  probe icmp-probe
  inservice
rserver host webserver3
  ip address 10.4.49.113
  conn-limit max 4000000 min 4000000
  probe icmp-probe
  inservice
rserver host webserver4
  ip address 10.4.49.114
  conn-limit max 4000000 min 4000000
  probe icmp-probe
  inservice

serverfarm host appfarm
  probe http-probe
  rserver webserver3 80
    conn-limit max 4000000 min 4000000
    inservice
  rserver webserver4 80
    conn-limit max 4000000 min 4000000
    inservice
serverfarm redirect http-redirect
  rserver redirect1
    conn-limit max 4000000 min 4000000
    inservice
serverfarm host webfarm
  probe http-probe
  inband-health check log 5 reset 500
  retcode 404 404 check log 5 reset 10
  retcode 500 505 check log 5 reset 10
  rserver webserver1 80
    conn-limit max 4000000 min 4000000
    inservice
  rserver webserver2 80
    conn-limit max 4000000 min 4000000
    inservice

sticky http-cookie APPSESSIONID app-sticky
  cookie insert browser-expire
  serverfarm appfarm


ssl-proxy service app-ssl-proxy
  key cisco-sample-key
  cert cisco-sample-cert
```

```
class-map type http loadbalance match-any default-compression-
exclusion-mime-type
  description DM generated classmap for default LB compression
exclusion mime types.
  2 match http url .*gif
  3 match http url .*css
  4 match http url .*js
  5 match http url .*class
  6 match http url .*jar
  7 match http url .*cab
  8 match http url .*txt
  9 match http url .*ps
  10 match http url .*vbs
  11 match http url .*xsl
  12 match http url .*xml
  13 match http url .*pdf
  14 match http url .*swf
  15 match http url .*jpg
  16 match http url .*jpeg
  17 match http url .*jpe
  18 match http url .*png
class-map match-all http-vip
  2 match virtual-address 10.4.49.100 tcp eq www
class-map match-all http-vip-redirect
  2 match virtual-address 10.4.49.101 tcp eq www
class-map match-all https-vip
  2 match virtual-address 10.4.49.101 tcp eq https
class-map type management match-any remote_access
  2 match protocol xml-https any
  3 match protocol icmp any
  4 match protocol telnet any
  5 match protocol ssh any
  6 match protocol http any
  7 match protocol https any
  8 match protocol snmp any

policy-map type management first-match remote_mgmt_allow_policy
  class remote_access
    permit

policy-map type loadbalance first-match http-vip-l7slb
  class default-compression-exclusion-mime-type
    serverfarm webfarm
  class class-default
    serverfarm webfarm
    compress default-method deflate
policy-map type loadbalance first-match http-vip-redirect-l7slb
  class class-default
    serverfarm http-redirect
policy-map type loadbalance first-match https-vip-l7slb
  class default-compression-exclusion-mime-type
    sticky-serverfarm app-sticky
  class class-default
    compress default-method deflate
    sticky-serverfarm app-sticky

policy-map multi-match int149
  class https-vip
    loadbalance vip inservice
    loadbalance policy https-vip-l7slb
    nat dynamic 1 vlan 149
    ssl-proxy server app-ssl-proxy
  class http-vip-redirect
    loadbalance vip inservice
    loadbalance policy http-vip-redirect-l7slb
  class http-vip
    loadbalance vip inservice
    loadbalance policy http-vip-l7slb
    nat dynamic 1 vlan 149

interface vlan 149
  ip address 10.4.49.120 255.255.255.0
  peer ip address 10.4.49.119 255.255.255.0
```

```
  access-group input ALL
  nat-pool 1 10.4.49.99 10.4.49.99 netmask 255.255.255.0 pat
  service-policy input remote_mgmt_allow_policy
  service-policy input int149
  no shutdown

ft interface vlan 912
  ip address 10.255.255.2 255.255.255.0
  peer ip address 10.255.255.1 255.255.255.0
  no shutdown

ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 912
ft group 1
  peer 1
  associate-context Admin
  inservice

ip route 0.0.0.0 0.0.0.0 10.4.49.1

snmp-server community ***** group Network-Monitor


username admin password 5 ***** role Admin domain default-domain
username www password 5 ***** role Admin domain default-domain
```

Notes

Appendix A: Product List

Data Center Core

Functional Area	Product Description	Part Numbers	Software
Core Switch	Cisco Nexus 5596 up to 96-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5596UP-FA	NX-OS 5.2(1)N1(1b) Layer 3 License
	Cisco Nexus 5596 Layer 3 Switching Module	N55-M160L30V2	
	Cisco Nexus 5548 up to 48-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5548UP-FA	
	Cisco Nexus 5548 Layer 3 Switching Module	N55-D160L3	
Ethernet Extension	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T (enhanced) Fabric Extender	N2K-C2248TP-E	—
	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender	N2K-C2248TP-1GE	
	Cisco Nexus 2000 Series 32 1/10 GbE SFP+, FCoE capable Fabric Extender	N2K-C2232PP-10GE	

Data Center Services

Functional Area	Product Description	Part Numbers	Software
Application Resiliency	Cisco ACE 4710 Application Control Engine 2Gbps	ACE-4710-02-K9	A5(1.2)
	Cisco ACE 4710 Application Control Engine 1Gbps	ACE-4710-01-K9	
	Cisco ACE 4710 Application Control Engine 1Gbps 2-Pack	ACE-4710-2PAK	
	Cisco ACE 4710 Application Control Engine 500 Mbps	ACE-4710-0.5-K9	
Firewall	Cisco ASA 5585-X Security Plus IPS Edition SSP-40 and IPS SSP-40 bundle	ASA5585-S40P40-K9	ASA 9.0(1) IPS 7.1(6) E4
	Cisco ASA 5585-X Security Plus IPS Edition SSP-20 and IPS SSP-20 bundle	ASA5585-S20P20X-K9	
	Cisco ASA 5585-X Security Plus IPS Edition SSP-10 and IPS SSP-10 bundle	ASA5585-S10P10XK9	

Storage Network Extension

Functional Area	Product Description	Part Numbers	Software
Fibre-channel Switch	Cisco MDS 9148 Multilayer Fibre Channel Switch	DS-C9148D-8G16P-K9	NX-OS 5.0(8)
	Cisco MDS 9124 Multilayer Fibre Channel Switch	DS-C9124-K9	

Computing Resources

Functional Area	Product Description	Part Numbers	Software
UCS Fabric Interconnect	Cisco UCS up to 48-port Fabric Interconnect	UCS-FI-6248UP	2.1(1a) Cisco UCS Release
	Cisco UCS up to 96-port Fabric Interconnect	UCS-FI-6296UP	
UCS B-Series Blade Servers	Cisco UCS Blade Server Chassis	N20-C6508	2.1(1a) Cisco UCS Release
	Cisco UCS 8-port 10GbE Fabric Extender	UCS-IOM2208XP	
	Cisco UCS 4-port 10GbE Fabric Extender	UCS-IOM2204XP	
	Cisco UCS B200 M3 Blade Server	UCSB-B200-M3	
	Cisco UCS B200 M2 Blade Server	N20-B6625-1	
	Cisco UCS B250 M2 Blade Server	N20-B6625-2	
	Cisco UCS 1280 Virtual Interface Card	UCS-VIC-M82-8P	
	Cisco UCS M81KR Virtual Interface Card	N20-AC0002	
UCS C-Series Rack-mount Servers	Cisco UCS C220 M3 Rack Mount Server	UCSC-C220-M3S	1.4.6 Cisco UCS CIMC Release
	Cisco UCS C240 M3 Rack Mount Server	UCSC-C240-M3S	
	Cisco UCS C200 M2 Rack Mount Server	R200-1120402W	
	Cisco UCS C210 M2 Rack Mount Server	R210-2121605W	
	Cisco UCS C250 M2 Rack Mount Server	R250-2480805W	
	Cisco UCS 1225 Virtual Interface Card Dual Port 10Gb SFP+	UCSC-PCIE-CSC-02	
	Cisco UCS P81E Virtual Interface Card Dual Port 10Gb SFP+	N2XX-ACPCI01	

Feedback

Please use the feedback form to send comments and suggestions about this guide.

SMART BUSINESS ARCHITECTURE

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

B-0000505-1 1/13