Capítulo 12

REDES INALÁMBRICAS IEEE 802.11 A/B/G

Para que una estación cliente (inalámbrica) tenga acceso a la infraestructura de red, es necesario que ésta se asocie y autentique con el punto de acceso (Access Point) que se encuentre más cercano. Las soluciones de acceso inalámbrico IEEE 80.2.11, en general, pueden basarse en un conjunto de puntos de acceso autónomos o en un conjunto de puntos de acceso livianos (administrados por un controlador central), distribuidos estratégicamente en las áreas que requieran el servicio. La conexión entre la estación cliente y el punto de acceso (AP) puede ser abierta o proporcionar diferentes grados de seguridad: WEP, WPA o WPA2 (personal o empresarial). En el presente capítulo se aborda el aprovisionamiento de tres puntos de acceso autónomos (AP1, AP2 y AP3) que usan las normas IEEE802.11 b/g, y coexisten en la misma área de trabajo gracias a que operan en los canales 1, 6 y 11, respectivamente. También se aborda el aprovisionamiento de una red inalámbrica con mayor cobertura, en la cual se utiliza la interfaz de radio IEEE 802.11a para el enlace entre AP1 y AP2, y se reutiliza la interfaz de radio IEEE 802.11 b/g para el enlace entre el AP1 y AP3. La seguridad que se utiliza en los diferentes enlaces es: abierta, WEP, WPA personal y WPA2 personal.

Objetivo

Al finalizar este capítulo, el estudiante estará en capacidad de:

- Configurar un punto de acceso inalámbrico y las estaciones clientes inalámbricas (IEEE 802.11 b/g) para que funcionen "sin seguridad" o con seguridad "WEP open".
- Configurar un punto de acceso inalámbrico y las estaciones clientes inalámbricas (IEEE 802.11 b/g) para que funcionen con "WPA personal (TKIP o AES) usando clave compartida".
- Realizar la interconexión de varias redes inalámbricas mediante puntos de acceso IEEE 802.11 a/b/g.

Procedimiento

Configuración de los puntos de acceso inalámbricos y de las estaciones clientes inalámbricas IEEE 802.11 b/g

Identificación de los equipos a usar en el montaje

Un punto de acceso inalámbrico es un dispositivo que funciona en la capa 2, sus decisiones las basa en las direcciones MAC, presentes en las tramas Ethertnet (o IEEE 802.3) de la parte cableada y en las tramas IEEE 802.11 del lado inalámbrico de la red. Después que la estación cliente inalámbrica, se haya asociado y autenticado con el AP, este último recibirá las tramas "unicast" de dicha estación (aquellas tramas que tengan como destino una estación en la red cableada) y las reenviará hacia la red alambrada. El AP también recibirá las tramas "unicast" de la red alambrada (que tengan como destino la estación inalámbrica) y las reenviará hacia a la estación inalámbrica. Para el caso de las tramas de difusión (broadcast), el AP se comporta como un dispositivo de capa 2 convencional.

Para el montaje, se dispone de los puntos de acceso relacionados en la Tabla 12.1. Es provechoso tomar nota de las direcciones MAC que tienen las interfaces alambradas y las interfaces de aire de cada dispositivo, puesto que esto facilita el entendimiento y verificación de los resultados. En la Tabla 12.1 se asigna una dirección IP a la interfaz BVI1 de cada AP con el propósito de habilitar su administración. El AP utilizado tiene la interfaz IEEE 802.11 b/g (antena de 2.4 Ghz) en el mismo lado que la interfaz FastEthernet (parte frontal de la Figura 12.1), mientras que la interfaz IEEE 802.11a (antenas de 5 Ghz) está en el lado opuesto (parte posterior de la Figura 12.1).

Tabla 12.1 Direcciones MAC correspondientes a las interfaces LAN y de aire de los puntos de acceso

Punto de acceso *Modelo del AP* *Hostname del AP* *Dirección IP de BVI1*	**Interfaz FastEthernet 0** *Dirección MAC*	**Interfaz Dot11Radio0** **IEEE 802.11 b/g** *Canal de operación* *Dirección MAC*	**Interfaz Dot11Radio1** **IEEE 802.11a** *Canal de operación* *Dirección MAC*
AIR-AP1242AG-AK9 ap1 192.168.55.150	0018:b9e9:4aaa	1 0018:7489:ec70	Dinámico 0018:748d:ec70
AIR-AP1242AG-AK9 ap2 192.168.55.151	0018.b9e9.4b7e	6 0018.7489.f310	Dinámico 0018.748d.f310
AIR-AP1231G-AK9 ap3 192.168.55.152	0018.19bd.b6a7	11 000a.b87e.b680	N/A N/A

Figura 12.1. Punto de acceso inalámbrico modelo AIR-AP1242AG-A-K9 de Cisco™

Una estación inalámbrica que se asocie a un AP puede recibir una dirección IP de parte de un servidor DHCP instalado en la red alambrada, o puede tener asignada la dirección IP de manera permanente. Para el montaje se dispone de las tarjetas inalámbricas USB relacionadas en la Tabla 12.2, cada interfaz inalámbrica tiene una dirección MAC asignada por el fabricante (la cual se puede administrar localmente).

Figura 12.2. Tarjeta USB inalámbrica WUSB54GC marca Linksys (Cisco)

Tabla 12.2. Direcciones MAC correspondientes a las tarjetas inalámbricas WUSB54GC

Nombre del equipo	Dirección MAC de la tarjeta inalámbrica
PC-A	0018:3917:91fd
PC-B	0018:3917:918f
PC-C	0018:3917:9180
PC-D	0018:3917:91ba

Instalar el driver de las tarjetas inalámbricas y la tarjeta WUSB54GC

Siga el siguiente procedimiento en estricto orden (no conecte la tarjeta WUSB54GC al computador personal antes de instalar el driver).

1. Usando el CD de las tarjetas WUSB54GC, instale el driver en los computadores personales: PC-A, PC-B, PC-C, PC-D.
2. Ahora ya puede conectar la tarjeta WUSB54GC a cada computador personal
3. Desconecte estos cuatro PC de la red local alambrada (Ethernet).

Configurar tres puntos de acceso con los valores por defecto, configurar la dirección IP en la interfaz BVI1, entrar a "Express Setup" por medio de un navegador Web, configurar un servidor DHCP, habilitar las interfaces de radio y configurar los canales de operación de la interfaz de radio 802.11 b/g

1. Manteniendo presionado el botón "mode" del "Access Point" (estando el AP apagado), simultáneamente conecte el adaptador a un tomacorriente durante 2 minutos. Repita este paso para cada uno de los tres AP.

2. Conecte el puerto COM1 del PC al puerto de consola del AP. Use un programa de emulación de terminal (por ejemplo, el programa Hyperterminal: 9600, 8, ninguno, 1, ninguno) para entrar a la interfaz de línea de comandos de cada AP (ap1, ap2 ó ap3) y verificar la configuración actual mediante el comando *show running-config*; constate que las interfaces de radio estén administrativamente deshabilitadas (shutdown).
3. Configure el "hostname" y la dirección IP de la interfaz BVI1 de cada AP de la siguiente manera (digite el usuario "Cisco" y la clave "Cisco").

```
ap> enable
password: Cisco
ap# show running-config
ap# configure terminal
(config)# hostname ap1 !(o ap2 o ap3, nombre de acuerdo a la Tabla 12.1)
(config)# interface BVI1
(config-if)# ip address 192.168.55.150 255.255.255.0 !(valor de acuerdo a la Tabla 12.1)
```

4. Conecte la interfaz FastEthernet 0 de cada AP (interfaz de LAN alambrada del AP) a los puertos de un conmutador Ethernet (puertos que pertenezcan a la VLAN 1, en el supuesto caso que el conmutador tenga configuradas varias VLAN). Mediante otro computador que se encuentre conectado al conmutador, ejecute un programa navegador Web (Mozilla Firefox o Internet Explorer) y acceda a cada AP (use la dirección URL http://192.168.55.150 para el ap1, http://192.168.55.151 para el ap2, http://192.168.55.152 para el ap3), digite el usuario "Cisco" y la clave "Cisco". Haga clic en la opción "Express Setup" y configure la puerta de enlace de cada AP con la dirección 192.168.55.106, hacer clic en "Apply".
5. Configurar solamente el ap1 para que haga la función de servidor DHCP.

```
ap1(config)# ip dhcp excluded-address 192.168.55.1 192.168.55.220
ap1(config)# ip dhcp pool direcciones
ap1(config-pool)# network 192.168.55.0 255.255.255.0
ap1(config-pool)# default-router 192.168.55.106
ap1(config-pool)# lease 1
ap1(config-pool)# dns-server 192.168.18.10
```

6. Habilitar las interfaces de radio 802.11 b/g en cada AP (en ap1, ap2 y ap3).

(config)# *interface Dot11Radio0*
(config-if)# *no shutdown*

7. Habilitar las interfaces de radio 802.11 a en cada AP (solamente en ap1 y ap2).

(config*)# interface Dot11Radio1*
(config-if)# *no shutdown*

8. Para evitar interferencia entre las interfaces 802.11 b/g de los AP, hay que configurarlos para que el ap1 funcione utilizando el canal 1, el ap2 utilice el canal 6 y al el ap3 utilice el canal 11. Esto se consigue por medio del navegador Web, al hacer clic en la opción "Network Interfaces" (que permite observar la página resumen de interfaces); después, hacer clic en la interfaz de radio "Radio802.11B/G" (que permite observar la página que muestra el estado de la interfaz de radio), hacer clic en la pestaña "Settings" (que permite observar la página de configuración de la interfaz de radio), "seleccionar el canal" de la interfaz de radio 802.11 b/g (de acuerdo al nombre del AP en la Tabla 12.1) y hacer clic en "Apply".

Configuración para operar en modo "No security"

1. Hacer clic en la opción "Express Security", crear un SSID (Service set identifier) en cada AP con las siguientes características:

   Nombre: ap1nosec (para el ap1), ap2nosec (para el ap2), ap3nosec (para el ap3).

   - Que no pertenezca a ninguna VLAN.
   - Que sea difundido en la trama de "Beacon".
   - Sin seguridad.

   Cuando se usa la opción "Express Security", por defecto, el SSID creado es aplicado a ambas interfaces de radio, a pesar que el usuario requiera aplicar el SSID a una sola interfaz de radio. En nuestro caso, nos interesa que el SSID sea aplicado a la interfaz de radio Dot11Radio0 (802.11 b/g). Lo anterior se traduce a las siguientes líneas del archivo de configuración en la interfaz Dot11Radio0 para el ap1.

```
! El comando “guest-mode” difunde el SSID ap1nosec en la trama Beacom
dot11 ssid ap1nosec
 authentication open
 guest-mode
!
interface Dot11Radio0
 !
 ssid ap1nosec
```

2. En los computadores personales (PC-A, PC-B, PC-C, PC-D) con tarjetas WUSB54GC, hacer un barrido para buscar las redes inalámbricas anunciadas por los AP. Para uno de los SSID anunciados, modificar su perfil en el software de la tarjeta USB, haciendo que el nombre del SSID configurado coincida con el SSID anunciado por el AP al cual se desea conectar, y configurar la opción “security = disable”. Salvar la configuración y conectarse al AP. Verificar que la tarjeta WUSB54GC del PC se asocia al AP correspondiente, recibe una dirección IP del servidor DHCP y puede comunicarse con otros equipos que se encuentran conectados a la red alambrada (mediante ping). Verificar las asociaciones con el comando *show dot11 assocciations*. Por medio de “Express Security”, borrar el SSID en los tres AP.

Configuración para operar en modo “WEP Open”

1. Hacer clic en la opción “Express Security”, crear un “SSID” en cada AP con las siguientes características:

   Nombre: ap1wepopen (para el ap1), ap2wepopen (para el ap2), ap3wepopen (para el ap3).

   - Que no pertenezca a ninguna VLAN.
   - Que el SSID sea difundido en la trama de Beacon.
   - Seguridad WEP Mandatory.
   - Clave en la ranura 1 para que tenga un tamaño de 40 bits con valor hexadecimal 0123456789 (Transmit Key).

   Lo anterior se traduce a las siguientes líneas del archivo de configuración en la interfaz Dot11Radio0 para el ap1.

```
dot11 ssid ap1wepopen
 authentication open
 guest-mode
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption key 1 size 40bit 7 BD5A59824B7D transmit-key
 encryption mode wep mandatory
 !
 ssid ap1wepopen
```

2. En los computadores personales (PC-A, PC-B, PC-C, PC-D) con tarjetas WUSB54GC, hacer un barrido para buscar las redes inalámbricas anunciadas por los AP. Para uno de los SSID anunciados, modificar su perfil en el software de la tarjeta USB, haciendo que el nombre del SSID configurado coincida con el SSID anunciado por el AP al cual se desea conectar, configurar la opción "security = WEP" y la clave con el valor 0123456789. Salvar la configuración y conectarse al AP. Verificar que la tarjeta WUSB54GC del PC se asocia al AP correspondiente, recibe una dirección IP del servidor DHCP y puede comunicarse con otros equipos que se encuentran conectados a la red alambrada (mediante ping). Por "Express Security" borrar el SSID.

Configuración para operar en modo
"WPA Personal TKIP con clave compartida"

1. Hacer clic en la opción "Security" y en "Encryption Manager" realizar los siguientes pasos:
   a. En "Encryption Mode" marcar "Cipher" y escoger "TKIP".
   b. Borrar el valor de la clave de cifrado 1.
   c. Marcar la clave de cifrado 2 como clave de transmisión.
   d. Aplicar lo anterior al radio Dot11Radio0.

2. En "SSID Manager" realizar los siguientes pasos:
   e. SSID = ap1tkip (para el ap1), ap2tkip (para el ap2), ap3tkip (para el ap3).
   f. Mediante el recuadro de selección aplicar el SSID al radio 802.11G.
   g. Marcar el recuadro de selección "Open authentication" y seleccione "No addition".

h. En la opción “Client Authentication Key Management”, seleccionar “Key Management = Mandatory”, marcar el recuadro “WPA”.
i. Llenar en “WPA Preshared Key” el valor “0123456789” y marcar el botón circular “ASCII”.
j. Aplicar la configuración con el primer botón “Apply”.

Lo anterior se traduce a las siguientes líneas del archivo de configuración en la interfaz Dot11Radio0 para el ap1.

```
dot11 ssid ap1tkip
 authentication open
 authentication key-management wpa
 wpa-psk ascii 7 055B575D72181B5F4E5D4E
!
interface Dot11Radio0
 encryption mode ciphers tkip
 !
 ssid ap1tkip
```

3. En los computadores personales (PC-A, PC-B, PC-C, PC-D) con tarjetas WUSB54GC, crear un perfil haciendo que el nombre del SSID configurado coincida con el SSID del AP al cual se desea conectar (el SSID no es anunciado porque no tiene el comando *guest-mode*), configurar la opción “security = WPA-Personal” y la clave compartida con el valor 0123456789. Salve la configuración y conéctese al AP. Verificar que la tarjeta WUSB54GC del PC se asocia al AP correspondiente, recibe una dirección IP del servidor DHCP y puede comunicarse con otros equipos que se encuentran conectados a la red alambrada (mediante ping). Por “Express Security” borrar el SSID en los tres AP.

Configuración para operar en modo “WPA Personal AES con clave compartida”

1. Hacer clic en la opción “Security” y en “Encryption Manager” realizar los siguientes pasos:
   a. En “Encryption Mode” marcar “Cipher” y escoger “AES-CCMP”.
   b. Borrar el valor de la clave de cifrado 1.
   c. Marcar la clave de cifrado 2 como clave de transmisión.
   d. Aplicar lo anterior al radio Dot11Radio0.

2. En “SSID Manager” realizar los siguientes pasos:
   e. SSID = ap1aes (para el ap1), ap2aes (para el ap2), ap3aes (para el ap3).
   f. Mediante el recuadro de selección, aplicar el SSID al radio 802.11G.
   g. Marcar el recuadro de selección “Open authentication” y seleccionar “No addition”.
   h. En la opción “Client Authentication Key Management”, seleccionar “Key Management = Mandatory”, marcar el recuadro “WPA”.
   i. Llenar en “WPA Preshared Key” el valor “0123456789” y marcar el botón circular “ASCII”.
   j. Aplicar la configuración.

   Lo anterior se traduce a las siguientes líneas del archivo de configuración en la interfaz Dot11Radio0 para el ap1.

```
dot11 ssid ap1aes
 authentication open
 authentication key-management wpa
 wpa-psk ascii 7 055B575D72181B5F4E5D4E
!
interface Dot11Radio0
 encryption mode ciphers aes-ccm
 ssid ap1aes
```

3. En los computadores personales (PC-A, PC-B, PC-C, PC-D) con tarjetas WUSB54GC, crear el perfil, haciendo que el nombre del SSID configurado coincida con el SSID del AP al cual se desea conectar (el SSID no es anunciado porque no tiene el comando *guest-mode*), configurar la opción “security = PSK2” y la clave compartida con el valor 0123456789. Salve la configuración y conéctese al AP. Verificar que la tarjeta WUSB54GC del PC se asocia al AP correspondiente, recibe una dirección IP del servidor DHCP y puede comunicarse con otros equipos que se encuentran conectados a la red alambrada (mediante ping). Por “Express Security” borrar el SSID.

Interconexión de los Puntos de acceso IEEE 802.11 a/b/g

En el siguiente montaje se busca que los puntos de acceso ap1 y ap2 se interconecten en modo punto a punto usando la interfaz de radio Dot11Radio1 de cada uno de ellos (IEEE802.11a, la cual opera a 5 Ghz). Para ello el ap1 opera en modo “root bridge” sobre su interfaz de radio Dot11Radio1,

mientras que el ap2 opera en modo “non-root bridge” sobre su interfaz de radio Dot11Radio1. Además el ap1 opera en modo “root bridge wireless-clients” sobre su interfaz de radio Dot11Radio0 (IEEE 802.11 b/g de 2.4 Ghz), con el fin de recibir tanto a las estaciones clientes cercanas como al ap3 por dicha interfaz, mientras que el ap3 opera en modo “non-root bridge with wireless clients” sobre su interfaz de radio Dot11Radio0 para recibir estaciones clientes cercanas y para asociarse al ap1.

Realizar el siguiente procedimiento general en el ap1

1. Configurar los siguientes SSID.

```
! SSID para aplicarlo a la interfaz Dot11Radio0 del ap1,
anunciarlo a los clientes del ap1 y ! recibir al ap3
dot11 ssid extendido
 authentication open
 guest-mode
!
! SSID para aplicarlo a la interfaz Dot11Radio1 del ap1 y recibir al ap2
dot11 ssid punto-a-punto
 authentication open
```

2. Hacer que la interfaz Dot11Radio0 funcione con WEP obligatorio, con la clave 1 de 40 bits de tamaño, valor hexadecimal de la clave igual a “0123456789”, que la clave 1 sea transmitida, aplicar el SSID “extendido” y que el papel de la interfaz sea “root bridge wireles-clients”.

```
interfaz Dot11Radio0
 !
 encryption key 1 size 40bit 7 BA94047C696A transmit-key
 encryption mode wep mandatory
 !
 ssid extendido
 !
 station-role root bridge wireles-clients
```

3. Hacer que la interfaz Dot11Radio1 funcione con WEP obligatorio, con la clave 1 de 40 bits de tamaño, valor hexadecimal de la clave igual a “9876543210”, que la clave 1 sea transmitida, aplicar el SSID “punto-a-punto” y que el papel de la interfaz sea “root bridge”.

```
interfaz Dot11Radio1
!
 encryption key 1 size 40bit 7 33072E76758A transmit-key
 encryption mode wep mandatory
 !
 ssid punto-a-punto
 !
 station-role root bridge
```

Realizar el siguiente procedimiento general en el ap2

1. Configurar los siguientes SSID.

```
! SSID para aplicarlo a la interfaz Dot11Radio0 del ap2 y anunciarlo a los clientes del
ap2
dot11 ssid remoto
 authentication open
 guest-mode
!
! SSID para aplicarlo a la interfaz Dot11Radio1 del ap2 y conectarse al ap1
dot11 ssid punto-a-punto
 authentication open
 infrastructure-ssid optional
```

2. Hacer que la interfaz Dot11Radio0 funcione con WEP obligatorio, con la clave 1 de 40 bits de tamaño, valor hexadecimal de la clave igual a “1234512345”, que la clave 1 sea transmitida, aplicar el SSID “remoto” y que el papel de la interfaz sea “root”.

```
interface Dot11Radio0
 !
 encryption key 1 size 40bit 7 66061D6FD052 transmit-key
 encryption mode wep mandatory
 !
 ssid remoto
 !
 station-role root
```

3. Hacer que la interfaz Dot11Radio1 funcione con WEP obligatorio, con la clave 1 de 40 bits de tamaño, valor hexadecimal de la clave igual a

"9876543210", que la clave 1 sea transmitida, aplicar el SSID punto-a-punto y que el papel de la interfaz sea "non-root bridge".

```
interface Dot11Radio1
!
 encryption key 1 size 40bit 7 EE6B241F059D transmit-key
 encryption mode wep mandatory
 !
 ssid punto-a-punto
 !
 station-role non-root bridge
```

Realizar el siguiente procedimiento general en el ap3.

1. Configurar el siguiente SSID.

```
! SSID para aplicarlo a la interfaz Dot11Radio0 del ap3,
anunciarlo a los clientes del ap3 y ! conectarse al ap1
dot11 ssid extendido
 authentication open
 guest-mode
 infrastructure-ssid optional
```

2. Hacer que la interfaz Dot11Radio0 funcione con WEP obligatorio, con la clave 1 de 40 bits de tamaño, valor hexadecimal de la clave igual a "0123456789", que la clave 1 sea transmitida, aplicar el SSID "extendido" y que el papel de la interfaz sea "non-root bridge wireles-clients".

```
interface Dot11Radio0
 !
 encryption key 1 size 40bit 7 66063D6FD042 transmit-key
 encryption mode wep mandatory
 !
 ssid extendido
 !
 station-role non-root bridge wireles-clients
```

Problemas

1. Buscar una solución inalámbrica de un fabricante (Cisco, Meru Networks, Aruba Networks, Trapeze) que incluya los pasos necesarios para el aprovisionamiento de una red basada en puntos de acceso livianos manejados desde un controlador central o WLC (Wireless LAN Controller).
2. Leer sobre los aspectos generales y el estado actual del protocolo estándar de control y aprovisionamiento de puntos de acceso inalámbricos (CAPWAP: Control And Provisioning of Wireless Access Points Protocol Specification, RFC 5415).

Glosario

Asociarse: primer paso que se da en el establecimiento de la conexión entre una estación cliente inalámbrica y un punto de acceso (que emite uno o varios identificadores o SSID). El usuario de la estación cliente decide con cuál identificador desea asociarse para continuar con el establecimiento de la conexión.

Autenticarse: segundo paso que se da en el establecimiento de la conexión entre una estación cliente inalámbrica y un punto de acceso. En este paso, la estación presenta las credenciales para que el punto de acceso las valide y permita el flujo de tramas con datos hacia y desde la red cableada.

SSID (Service Set Identifier): identificador emitido por la interfaz de radio del punto de acceso (el AP puede emitir uno o varios SSID). El SSID tiene un perfil que define las características que tendrá la conexión de la estación cliente inalámbrica que se autentique en dicho identificador (VLAN, usuario, clave, etc.).

Trama Beacon: trama de gestión IEEE 802.11 que se emite con cierta periodicidad (100 milisegundos por lo general, o el valor configurado), anunciando la presencia de la red inalámbrica e información de la red.

Unicast: tramas o paquetes que van dirigidos a un solo destino.

WEP (Wired Equivalent Privacy): algoritmo de seguridad (frágil) usado para proteger un enlace IEEE 802.11, caracterizado por usar una clave con longitud de 40 bits o de 104 bits. Declarado obsoleto por la IEEE en el año 2004.

WPA (Wi-Fi Protected Access) Personal: algoritmo de seguridad (intermedio) usado para proteger un enlace IEEE 802.11, útil en equipos que no tengan hardware con soporte WPA2. WPA Personal está basado en el

protocolo de cifrado TKIP (Temporal Key Integrity Protocol) y en una clave compartida entre el punto de acceso y la estación cliente.

WPA2 Personal o Empresarial: algoritmo de seguridad (sucesor de WPA) usado para proteger un enlace IEEE 802.11. Está basado en un mecanismo de cifrado AES y usa el protocolo CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).

Bibliografía

GAST, M. (2002). *802.11 Wireless Networks: The Definitive Guide*. Sebastopol, CA: O'Reilly.

KOTFILA, D.; MOORHOUSE, J.; PRICE, C.; WOLFSON, R. (2008) *CCNP Building Multilayer Switched Networks (BCMSN 642-812) Lab Portfolio*. Indianapolis, IN: Cisco Press.