

BCMSN

This is my personal summary of what I believe are the key points of needed to pass Cisco's BCMSN test. I have no special insight into the test (other than years of teaching the course material.) This summary is not endorsed by ANYONE. This summary represents a minimum base of knowledge for the BCMSN test. You should know MORE than this before taking the test!

This material is provided freely for individual, non-commercial use. Any and all commercial use is prohibited. All rights are reserved by TrainingMagic, inc. and the author, Bob Cunningham.

Remember that the BCMSN is a test of skill as well knowledge. Make sure that you know ALL of the facts listed here and be able to configure ALL of the applications listed here.

Module 1

Designing Networks using the Campus Infrastructure Module

Flat networks have: large collision domains, large broadcast domains, high latency and are difficult to troubleshoot.

Hubs are layer 1 devices, switches are layer 2 devices and routers are layer 3 devices.

Switches break up collision domains and have a single collision domain per port.

Routers break up broadcast domains; have a single broadcast domain per port and use ACLs to filter traffic between segments. Also, routers have a high per port cost and high latency compared to layer 2 switches.

A layer 3 switch combines router and switch functions on the same box with low latency.

Potential Problems with Multilayer switches include; hardware being underutilized if used simply as a replacement for a router, a single point of failure and increased complexity when spanning tree is used.

The hierarchical campus model has 3 layers: Access, Distribution and Core.

The access layer provides access to the network and breaks up broadcast domains.

The distribution layer provides policy based connectivity like security, QOS and uses ACLs.



The core layer (aka campus backbone) provides high speed/low latency switching.

There are 3 functional areas of the enterprise composite model. In addition to the Enterprise Campus, there are two other areas; Enterprise Edge and Service provider Edge.

Example services in these areas include:

Enterprise Campus – Building Core, Building Distribution, Building Access

Enterprise Edge – DMZ, Firewall & AAA

Service Provider Edge – WAN services

Problems with poor network design include:

Unbounded failure domains

Large broadcast domains

Large amount of unknown MAC unicast traffic

Unbounded multicast traffic

Management and support challenges

Possible security vulnerabilities

The benefits of scaleable network addressing include; Ease of management & troubleshooting by using a well known scheme, minimizing IP configuration errors, small routing table entries.

Best practices for network addressing include; assign network addresses contiguously from the distribution to access, use one subnet per VLAN and avoid VLSM.

Best practices for bandwidth aggregation include; Plan for growth - 30 % above planned capacity recommended, use the following oversubscription ratios:

Access to Distribution 20:1

Distribution to Core 4:1

Core to Core 1:1

Best practices for VLAN design include:

One VLAN to each Subnet

Routing between VLANs done at Distribution layer

End user VLANs limited to an Access switch

Use a separate VLAN for each class

Scavenger class can be for "misc." categories



Module 2

Implementing VLANs

In End-to-End VLANs users are grouped into VLANs independent of physical location and this design is based on the OLD 80/20 rule.

With Local VLANs users are generally confined to a wiring closet and design is based on the NEW 20/80 rule.

There are two modes used to create VLANs - Global & Database – Global Mode is preferred.

Global VLAN Configuration Mode:

```
Switch# configure terminal
Switch(config)# vlan 3
Switch(config-vlan)# name Vlan3
Switch(config-vlan)# exit
Switch(config)# end
```

Database VLAN Configuration Mode (This mode is being deprecated):

```
Switch# vlan database
Switch(vlan)# vlan 3
```

```
VLAN 3 added:
Name: VLAN0003
Switch(vlan)# exit
```

The benefits of local VLANs in the Enterprise Composite Network Model:

- Deterministic traffic flow
- Finite failure domain
- High availability
- Ease of management

To assign a VLAN to a port, 1st place the port in access mode then apply the VLAN.

```
(config)#interface FastEthernet 0/17
(config-if)#switchport mode access
(config-if)#switchport access vlan 3
```

Verify VLAN configuration with the *show interface* or *show vlan* commands.



Trunks carry all VLANs by default. Access ports are associated with only a single VLAN.

Be able to compare ISL and 802.1Q

ISL	802.1Q
Proprietary	Nonproprietary
Encapsulated (26 B header/4 B trailer) Ethernet Frame is NOT modified	Tagged Ethernet Frame is modified (tag & crc)
Protocol independent	Protocol dependant
Encapsulates the old frame in a new frame	Adds a field to the frame header

The 802.1q tag is inserted into an Ethernet frame following the source MAC address. The two byte tag contains 3 bits used to indicate the priority of the frame (in accordance with the 802.1p standard), 1 bit used if passing data from Token ring to Ethernet and 12 bits used for a VLAN ID.

In 802.1Q untagged Ethernet is called the native VLAN and is used to support hardware or protocols that do not support 802.1Q VLANs. By Default all switch ports are assigned to the native VLAN. By Default the native VLAN is VLAN 1.

Potential native VLAN problems:

- Native VLAN must match at ends of trunk.
- A mismatch could cause layer 2 loops .
- CDP may have issues over native VLAN if the native VLAN is not VLAN 1.

VLAN Range	Use
0, 4095	Reserved for system use only
1	Cisco default
2–1001	For Ethernet VLANs
1002–1005	Cisco defaults for FDDI and Token Ring
1006–4094	Ethernet VLANs only, unusable on specific legacy platforms

Trunks carry all VLANs by default: Dynamic Trunking Protocol automatically configures ports in trunking mode or access mode.



Know the combinations of DTP states and the port states they will result in.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Not recommended
Access	Access	Access	Not recommended	Access

Be able to configure a trunk on a Cisco switch:

```
Switch(config)#interface fastethernet 2/1
Switch(config-if)#shutdown
Switch(config-if)#switchport trunk encapsulation (isldot1q)
Switch(config-if)#switchport trunk allowed vlan 1-5,1002-1005
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#switchport mode trunk [dynamic(autodesirable)]
Switch(config-if)#switchport nonegotiate
Switch(config-if)#no shutdown
```

Remember that the encapsulation command is not available on desktop switches.

Be able to verify trunk configuration via the “show running-config” *or* “the show interface switchport *type module/port*” command.

In order to form a trunk make sure that:

- the Layer 2 interface mode configured on both ends of the link is valid
- the trunk encapsulation type configured on both ends of the link is valid
- the native VLAN is the same on both ends of the trunk (802.1Q trunks)
- the Switches are in same VTP domain

VLAN Trunking Protocol

VTP propagates consistent VLAN information between switches that are part of the same management are (known as a VTP domain).

Switches running VTP are in one of three modes:

- Server** which can -
 - Creates, modifies, and deletes VLANs
 - Sends and forwards advertisements
 - Synchronizes VLAN configurations
 - Saves configuration in NVRAM



Client which can -

- Cannot create, change, or delete VLANs
- Forwards advertisements
- Synchronizes VLAN configurations
- Does not save information in NVRAM

Transparent which turns off VTP and has these characteristics –

- Creates, modifies, and deletes local VLANs
- Forwards advertisements
- Does not synchronize VLAN configurations
- Saves configuration in NVRAM

Know the 3 versions of VTP:

- Version 1** Original Flavor
- Version 2** Supports Token Ring
Checks for Consistency of VTP and VLAN information
Not interoperable with Version 1
- Version 3** Supports extended VLAN addresses
Supports Private VLANs & MST
Interoperable with Versions 1 & 2

Know the 3 types of VTP advertisements:

- Summary Advertisement** - sent every 5 Minutes
- Advertisement Requests** - sent to server if Summary conflicts w/ database
- Subset Advertisement** - set per changed vlan in response to Advert Req

Be able to set a VTP Domain, VTP Password, VTP mode and VTP pruning.

- Switch(config)#vtp domain** *domain name*
- Switch(config)#vtp password** *password*
- Switch(config)#vtp mode** (*server|client| transparent*)
- Switch(config)#vtp pruning**

VTP pruning removes broadcast traffic off of a trunk that has no downstream clients for that vlan. VTP pruning is on by default.

Cisco switch are in VTP server mode by default.

Verify VTP configuration with “show vtp status” and “show vtp counters”

An unconfigured switch will “learn the first domain name it sees”.



When inserting a switch into a network best practice suggests placing the switch in a different domain and in transparent mode. Only after the switch is connected should you place the switch in server or client mode and enter the correct domain name.

Module 3

Spanning Tree

The 3 problems associated with layer 2 redundant paths are:

- Database instability
- Multiple frame transmission
- Broadcast storms

Spanning tree protocol (802.1D) provides loop free redundant topology.

A **Bridge ID** is made up of the switch Priority + the lowest MAC address on the switch.

The **root bridge** is the switch with the lowest Bridge ID and is the reference point for the entire switched network.

There is **one root port** per bridge, the root port has the lowest path cost from the bridge to the root bridge.

Each **LAN segment has one Designated Port** which provides the only path on the LAN segment to the Root Bridge.

All ports on a root switch are **designated**.

Non designated ports are **blocked**.

Switches learn the location of devices remembering the Source MAC addresses of an Ethernet frame as it enters the switch.

Switches flood Ethernet frames with unknown addresses to all ports.

Switches forward Ethernet frames with known addresses to the destination port only.

Filtering is when switches do not forward Ethernet frames with known addresses to ports other than destination port.

Store and forward switching reads the entire Ethernet frame and checks the CRC before forwarding it out the destination port.

Cut through reads the destination Ethernet MAC address and then immediately forwards the frame out the destination port.



Fragment free looks at the first 64 bytes of a frame to confirm that no collisions have occurred before forwarding the frame out the destination port.

Know the four states a spanning tree port transitions through

- Blocking** (receives BPDU's, asks "am I the root?")
- Listening** (sends, receives and PROCESSES BPDUs only – no Ethernet traffic)
- Learning** (creates a MAC database – does not forward)
- Forwarding** – acts like a full switch

Bridge Protocol Data Unit – BPDU

- BPDU's are sent out at the hello time interval (2 seconds by default)
- Only the root switch generates BPDU
- Only the root switch controls timers for the whole network

Bytes	Field
2	Protocol ID
1	Version
1	Message type
1	Flags
8	Root ID
4	Cost of path
8	Bridge ID
2	Port ID
2	Message age
2	Max age
2	Hello time
2	Forward delay

Bridge ID is made of two parts – Bridge Priority (2 Bytes) and MAC address (6 Bytes)
 - The default priority is 32768 – The MAC address is the lowest address on the switch

An **Extended Bridge ID** divides the 2 Byte Bridge priority field into two parts: a 4 bit bridge priority number and a 12 bit Extended ID field (which indicates the VLAN ID for use PVST+.)

Know the Spanning Tree Path Cost

Link Speed	Cost (Revised IEEE Spec)	Cost (Previous IEEE Spec)
10 Gbps	2	1
1 Gbp	4	1
100 Mbps	19	10
10 Mbps	100	100



Understand the **Root Bridge selection** process
 Understand the **Root Port selection** process
 Understand the **Designated Port selection** process

Understand the function of the Spanning Tree timers

Max age max time between hello bpdu transmissions - 6 to 40 (20 default)

(config)#spanning-tree vlan 10 max-age 24

Hello frequency of hellos - 1 to 10 (2 default)

(config)#spanning-tree vlan 10 hello-time 18

Frwd delay used in listening and learning - 4 to 30 (15 default)

(config)#spanning-tree vlan 10 forward-time 18

Cisco does not recommend changing these timers directly – instead change them indirectly by changing the network diameter using the root primary diameter command:

(config)#spanning-tree vlan 1 root primary diameter X

From the show spanning-tree output be able to determine the type of spanning tree protocol, root bridge ID, the priority number of the bridge, the system ID and any interface connected to an 802.1d switch.

#sh spanning-tree vlan 10

VLAN00010

Spanning tree enabled protocol rstp¹

Root ID Priority 4106

Address 0008.e3ce.3cc0

This bridge is the root²

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 4106³ (priority 4096⁴ sys-id-ext 10)

Address 0008.e3ce.3cc0

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p Peer(STP) ⁵
Fa0/7	Desg	FWD	19	128.7	P2p
Fa0/9	Desg	FWD	100	128.9	Shr
Fa0/11	Desg	FWD	19	128.11	P2p Peer(STP)
Fa0/12	Desg	FWD	19	128.12	P2p Peer(STP)
Fa0/15	Desg	FWD	100	128.15	Shr
Fa0/23	Desg	FWD	19	128.23	P2p



- 1) This bridge is running RSTP (802.1w) if it were 802.1d it would display ieee.
- 2) This is the root bridge
- 3) The priority of this bridge
- 4) The base priority which is the priority minus the vlan ID
- 5) This port is attached to an 802.1d switch

Set a switch as root by using the priority command or the root primary command and set a back up command using the root secondary command.

```
(config)#spanning-tree vlan 10 priority 4096
(config)#spanning-tree vlan 10 root primary
(config)#spanning-tree vlan 10 root secondary
```

PortFast immediately moves to the forwarding state and does not go through the blocking, listening, or learning states. This command should only be used on access ports where there is no chance of a loop.

```
(config-if)#spanning-tree portfast
```

EtherChannel

Logical aggregation of between 2 and 8 channels.

PAGP (Port Aggregation Protocol) is Cisco proprietary.

LACP (Link Aggregation Control Protocol) is an IEEE standard.

LACP Options

(config-if-range)#channel-group 1 mode on - Enable Etherchannel - no PAGP or LACP

(config-if-range)#channel-protocol lacp - Enables the IEEE standard protocol

(config-if-range)#channel-group 1 mode active - Enable LACP unconditionally

(config-if-range)#channel-group 1 mode passive - Enable if a LACP device is detected

PAGP Options

(config-if-range)#channel-protocol pagp - Enables the Cisco proprietary protocol

(config-if-range)#channel-group 1 mode desirable - Enable PAGP unconditionally

(config-if-range)#channel-group 1 mode auto - Enable PAGP if a PAGP device is detected



Configure Layer 2 EtherChannel

```
(config)#interface range interface slot/port - port
(config-if-range)#channel-protocol { pagp | lacp }
(config-if-range)#channel-group number mode { auto | desirable | on }
```

Configure Layer 3 EtherChannel

Assigns a port (or several ports) to a channel group:

```
(config)#interface interface slot/port
(config-if)#no switchport
(config-if)#channel-group number mode { auto | desirable | on }
```

Assign an IP address to a port-channel:

```
(config)#interface port-channel port-channel-number
(config-if)#no switchport
(config-if)#ip address address mask
```

EtherChannel Rules

Interfaces do not need to be contiguous.

Port costs can be different.

All interfaces must be in the same speed and duplex mode

One of the interfaces can not be an analyzer destination port.

All interfaces must have the same vlans assigned or be configured as trunks

IP address must be assigned to the logical port – not a physical interface

Port channel changes affect the EtherChannel.

Physical interface changes affect that interface only.

Set load balancing

```
(config)#port-channel load-balance (src-mac|dst-mac|src-dst-mac|src-ip|dst-ip|src-dst-ip)
```

Rapid Spanning Tree Protocol (RSTP)

RSTP combines Cisco proprietary improvements in STP in a IEEE standard.

RSTP ports exist in one of **three states**:

- Discarding
- Learning
- Forwarding



RSTP ports can be in one of **four** roles:

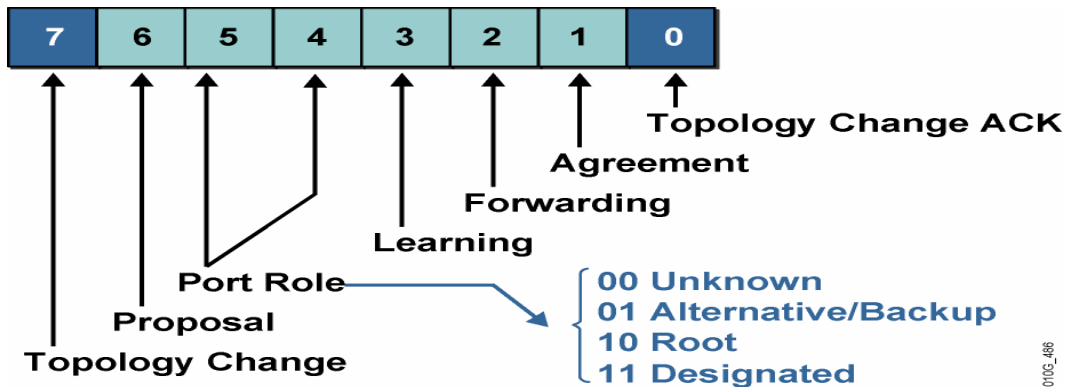
Root Port
 Designated Port
 Alternative Port
 Backup Port

RSTP edge port connect to a host – not another switch

Point-to-point links operate in full duplex.

Sharred links operate in half duplex mode.

RSTP redefines the flag byte:



The use of the **RSTP Proposal and Agreement bits** for rapid transition to forwarding has changed.

Rapid transition to forwarding is only achieved on edge ports and point-to-point links

- 1 - both ports in designated blocking when in blocking/learning sends out BPDU w/proposal bit
- 2 - Switch A receives a superior BPDU from ROOT. Switch A blocks non-edge ports (called synch)
- 3 - Switch A sends a BPDU w/agreement bit set – not the port in forwarding state

(config)#spanning-tree mode rapid-pvst sets 802.1w for the switch



Multiple Spanning Tree (MST) enables multiple VLANs to be mapped to the same spanning-tree instance. This reduces the number of spanning-tree instances on a switch and provides interoperability between PVST and 802.1d.

MST needs tree things configured on each switch:

- Name
- Revision number
- VLAN association table

MST uses the Extended System ID to carry the MST instance number

An MST region appears as a single virtual switch.

A special instance of MST runs in each MST region – The Internal Spanning-tree Instance (IST) it is always instance 0.

(config)#spanning-tree mst configuration – puts switch into mst configuration mode
(config-mst)#name *name*- configures an MST region name
(config-mst)#instance *inst* *vlan range*- Maps vlans into a region
(config-mst)#spanning-tree mst *instance_number* root *primary*|*secondary*

Module 4

Inter-vlan routing using multiple interfaces is suboptimal because:

- Routers are slow compared to switches
- Router ports are expensive

Router on a stick is better because it uses only a single port. However, routers are still slow and the switch router link may become congested.

```
(config)#interface Ethernet0/0
(config-f)# ip address 192.168.1.252 255.255.255.0
(config-f)#interface Ethernet0/0.2
(config-f)# encapsulation dot1Q 2
(config-f)# ip address 172.17.1.70 255.255.255.192
(config-f)#interface Ethernet0/0.3
(config-f)# encapsulation dot1Q 3
(config-f)# ip address 172.18.1.70 255.255.255.192
```

Route Caching = flowbased (route once, and switch many - see traffic flow then move to hardware)



Topology based = Cisco Express Forwarding (CEF) Use routing table to pre-create a hardware path

Centralized Switching (CEF) switches on the supervisory engine of a Cisco switch.

Distributed Switching (DCEF) switches on the blades providing faster switching.

FIB contains routing information it Caches Layer 3 Topology in CAM/TCAM

The adjacency table contains the next hop (layer 2) for all FIB entries

Adjacency table terms:

Glean State = there is a L2 network attached, but there is no entry for the specific host. Begin ARP Throttling

ARP Throttling drops packets until an ARP response is received

Punt Adjacency = Adjacencies that are not supported by L3 switching

Ternary Content Addressable Memory Matches based on three values: 0, 1, or X (either)

Turn on CEF

ip cef (enabled by default)

Turn on CEF on a VLAN

ip route-cache cef (only on VLAN interface)

Confirm CEF configuration

```
#show adjacency gigabitethernet 9/5 detail
#show interface {{type mod/port}} | {port-channel number}} | begin L3
#show interfaces {{type mod/port}} | {port-channel number}} include switched
```

A Switch Virtual Interface (SVI) applies Layer 3 functions to a VLAN

Sample configuration

```
(config)#ip routing
(config)#interface vlan 10
(config-if)#ip address 10.1.1.1 255.255.255.0
(config)#router eigrp 50
(config-router)#network 10.0.0.0
```



Routed Interfaces – Configures a physical switch port with Layer 3 capability

Sample configuration

```
(config)#interface FastEthernet 0/1
(config-if)#no switchport
(config-if)#ip address 10.1.1.1 255.255.255.0
(config)#router eigrp 50
(config-router)#network 10.0.0.0
```

Module 5

HSRP is a Cisco proprietary method of combining multiple routers into one virtual router. An HSRP virtual router presents a virtual IP and virtual MAC to hosts. One router in an HSRP group is active (i.e. processing all frames and packets sent to the virtual MAC address and the virtual IP address.) All other routers are in standby state.

Interpret a HSRP debug statement:

```
Id10h: SB10: Vlan5 Hello out 172.16.5.12 Active pri 150 hel 3 hol 10 ip 172.16.5.129
Hello from 172.16.5.12
This is the Active Router (other states include “Standby” and “Speak”)
It has a Priority of 150
The hello time is 3 sec.
The Hold time is 10 sec.
The Virtual IP is 172.16.5.129
```

An HSRP MAC address follows a predictable pattern: 0000.0c07.ac0b

0000.0c is a vendor code.

07.ac is a well known code identifying this as an HSRP virtual MAC address.

0b is the hexadecimal representation of the HSRP group 10.

An HSRP router can be in five states:

Initial - HSRP not running

Listen - Knows Virtual IP – not Active or Standby - Waits for hold time and listen for HSRP advertisements

Speak - Sends Hello messages

Standby - Router is in HSRP Standby state

Active - Router is in HSRP Active state



Create an HSRP group and assign a virtual IP
(config)standby 10 ip 172.16.5.129

Set priority for an HSRP router (100 is the default)
(config)standby 10 priority 150

Load balancing can be accomplished by **assigning routers to multiple groups** on the same subnet in a VLAN, or by **assigning routers multiple VLANs** or by **assigning routers to multiple groups in multiple VLANs**.

The Preempt command enables a router to resume the forwarding router role from a lower priority router.

(config)#standby 10 preempt

The hold timer should be at least 3 times the hello timer
(config-if)#standby 10 timers 5 15

Interface tracking reduces the priority of the by a specified number – the preempt command must also be configured.

(config)#standby 10 track GigabitEthernet 0/1 70

Virtual Router Redundancy Protocol (VRRP) is similar to HSRP but open standard – defined in RFC 2338.

Master Router presents a virtual IP and virtual MAC to hosts.
All other routers assume a backup role.

(config)#vrrp 10 ip 172.16.5.129
(config)#vrrp 10 priority 110
(config)#vrrp 10 timers advertise 4



Gateway Load Balancing Protocol (GLBP) is a Cisco Proprietary improvement over HSRP. In GLBP a single gateway IP address is shared by all routers. ARPs to the Virtual IP address are answered with the virtual MAC address of one of routers in the group in a "round robin" fashion. This fully utilizes resources on all routers in group.

The router that controls which vMAC is associated with which ARP request is called the Active Virtual Gateway (AVG). The router that is associated with a particular vMAC is called the Active Virtual Forwarder (AVF).

The GLBP can support up to 4 routers in a group, assures that traffic is proportionately load balanced between group members, and guarantees that the same vMAC will be used a host as long as that vMAC is participating in the GLBP group.

```
(config)#glbp 10 ip 172.16.5.129
(config)#glbp 10 priority 110
(config)#glbp 10 timers msec 200 msec 700
```

Module 6

Service Set Identifier (SSID) which are broadcast by Access point logically separate WLANs. Although Client can be configured without SSIDs, when configured, they are case sensitive.

A **Wireless Access Point (AP)** is the point at which wireless clients can access the wired network.

A **Wireless Repeater** is an access point that is not connected to the wired backbone.

A **Workgroup Bridge (WGB)** provides a wired connection to the wired network and provides a single wireless connection to an Access Point.

Ad Hoc mode provides peer-to-peer communications between wireless clients.

Layer 2 roaming allows clients to move between wireless cells in the same subnet.

Layer 3 roaming allows clients to move between wireless cells in different subnets.

Adaptive Wireless Path (AWP) protocol establishes an optimal path to root in a mesh network.



Understand the implications of **Shannon's Law**: $\text{Log}_2 * \text{BW} (\text{S/N} + 1)$

Higher Frequencies have shorter transmission distances.

	802.11b	802.11g		802.11a
Ratified	1999	2003		1999
Frequency band	2.4 GHz	2.4 GHz		5 GHz
No of channels	3	3		Up to 23
Transmission	DSSS	DSSS	OFDM	OFDM
Data rates [Mbps]	1, 2, 5.5, 11	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	6, 9, 12, 18, 24, 36, 48, 54
Throughput [Mbps]	Up to 6	Up to 22		Up to 28

802.11a	802.11b	802.11g
54Mbps nominal	11Mbps nominal	54Mbps nominal
5 Ghz carrier frequency	2.4Ghz carrier frequency	2.4Ghz carrier frequency
Less interference than b or g	More interference than a	More interference than a
Not compatible with b or g	Compatible with g	Compatible with b

Know the meaning of LED 0 and LED 1 for the CardBus and PCI cards:

- Power save mode: **Slow blink, off**
- Awake from power save mode: **On, off (can be used to indicate power is applied—the hardware automatically enters this state after exiting from power save mode before any other activity)**
- Looking for network association: **Alternate blink between LED 1 and LED 0**
- Associated or joined with network, no activity: **Slow simultaneous blink**
- Associated or joined with network, activity: **Fast simultaneous blink (blink rate increases with activity)**











Extensible Auth Protocol (EAP), Cisco Lightweight EAP (LEAP), and Protected EAP (PEAP) are all 802.1X authentication protocols that provide strong mutual authentication between the client and a RADIUS server.

Lightweight Access Point Protocol (**LWAPP**) protocol splits the function of the wireless MAC between a Wireless Access Point and a centralized WLAN controller.

Power Over Ethernet can be supplied by POE Switches or power injectors.

There are two methods of POE: **IEEE 802.3af & Cisco proprietary PoE**. New Cisco devices support both PoE methods

Know the states of the Aironet System Tray Utility Icon.

Desktop Logo	
ACU Status - Excellent	
ACU Status - Good	
ACU Status - Fair	
ACU Status - Poor	
ACU Status - No Radio	
ACU Status- Authenticating	
ACU Status- Not Associated	



dB is a logarithmic unit used to describe a ratio between input power and output power.

dBm is a decibel referenced to 1 milliwatt of power

dB*i* is the gain over theoretical isotropic.

Multipath distortion is a form of radio signal degradation that occurs when radio signals bounce off objects or surfaces causing the signals to add destructively.

Effective Isotropic Radiated Power (EIRP) is the Power coming off an antenna

36dBm is the MAX EIRP allowed by FCC regulation

EIRP [dBm] = Power [dBm] – cable_loss [db] + antenna_gain [dBi]

Module 7

Voice over IP (VoIP) packets are carried in RTP.

The maximum bandwidth usage for links carrying VoIP is 75%.

Call control signals are used to set up, maintain and tear down calls.

Digitized Voice traffic uses a relatively small amount of bandwidth and is relatively consistent in it's bandwidth. Voice is sensitive to delay and lost packets.

Data traffic is bursty, may require large amounts of bandwidth, is delay insensitive and relatively tolerant of lost packets.

The Auxiliary VLAN allows voice from a VOIP phone to be placed on a different VLAN from data on the same physical link with out having to assign different VLAN number on the phone itself.

Variable delay between successive packets is called jitter and is usually caused by queuing issues.

High availability networks are needed for VoIP. Requirements include UPS/generator support and 4 hour service-response time.

Use the "switchport voice vlan x" command to assign a VLAN number to the voice VLAN



Know these trust commands and their function:

mls qos trust cos

Instructs the device to trust the cos received on that port.

mls qos trust device cisco-phone

Instructs the port to trust the CoS received on the port if CDP detects a Cisco Phone

mls qos extend trust

Instructs the IP phone to trust the CoS value received from the PC attached to the phone.

switchport priority extend cos *cos_value*

Instructs the IP phone to override the CoS value received from the PC attached to the phone.

Understand all the commands and outputs in this display:

```
Switch(config)# mls qos
Switch(config)# interface fastethernet 0/4
Switch(config-if)# switchport voice vlan 110
Switch(config-if)# switchport access vlan 10
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos trust device cisco-phone
Switch(config-if)# ctrl-Z
Switch# show interfaces fastethernet 0/4
```

```
Switch# show mls qos interface fastethernet 0/4
```

```
FastEthernet0/4
trust state: trust cos
trust mode: trust cos
COS override: dis
default COS: 0
pass-through: none
trust device: cisco-phone
```

Know that “**Auto QOS**” automatically discovers applications and provides appropriate QoS treatment, automatically generates QoS policies, and supports Cisco IP Phone and Cisco IP Communicator

With “**Auto QOS**” the trust boundary is disabled when Cisco IP Phone is moved

“**Auto QOS**” is Supported on static, dynamic-access, voice VLAN, and trunk ports



CDP must be enabled for Cisco AutoQoS to function properly.

Use the “**Switch(config-if)# auto qos voip trust**” command when attached to a trusted switch or router.

Use the “**Switch(config-if)# auto qos voip cisco-phone**” command when attached to a Cisco VoIP phone.

Module 8

A MAC flood attack overloads the MAC Address table causing the switch to act like a hub. The port security max feature will prevent this.

Configure port security

```
(config)#interface fastethernet0/1
(config-if)#switchport mode access
(config-if)#switchport port-security
(config-if)#switchport port-security max 1
(config-if)#switchport port-security violation (protect/rest/shutdown)
(config-if)#switchport port-security mac-address sticky
```

VLAN hopping can be accomplished by an end host using DTP to fool the switch into changing the connection to the switch from access to trunk.

Configure non-trunk ports as access to disable DTP and prevent VLAN hopping.

```
(config-if)#switchport mode access
```

Private VLANs allow VLANs to talk to a promiscuous port but NOT with each other.

1 Define all the secondary VLANs that will be used. They can be isolated or community.

```
(config-vlan)# private-vlan {isolated | community}
```

2. Define the primary VLAN that will provide connectivity to the secondary VLANs.

```
(config-vlan)# private-vlan primary
(config-vlan)# private-vlan association {secondary-vlan-list | add
secondary-vlanlist | remove secondary-vlan-list}
```



Here is how to define and apply a VLAN access map to forward IP packets.

First define an access list

```
#access-list 11 permit 10.0.0.0 0.255.255.255
```

Second, create a VLAN Access Map

```
(config)# vlan access-map test 10  
(config-access-map)# match ip address 11  
(config-access-map)# action forward  
(config-access-map)# exit
```

Third, apply the Access Map to the appropriate VLANs

```
(config)# vlan filter test vlan-list 5-20
```

DHCP spoofing allows an attacker to respond to legitimate DHCP requests with the attacker's own information facilitating a man-in-the-middle attack.

DHCP snooping prevents DHCP spoofing attacks by establishing "trusted" and "untrusted" interfaces for DHCP offers.

Enable DHCP snooping globally:

```
(config)# ip dhcp snooping
```

Enable DHCP snooping on an interface:

```
(config-if)# ip dhcp snooping trust
```

Enable DHCP snooping on a VLAN:

```
(config)# ip dhcp snooping vlan number [number]
```

Option 82 allows DHCP to identify the port of origin of a DHCP message.

ARP spoofing is another way to facilitate a man-in-the-middle attack.

Dynamic ARP Inspection protects against ARP spoofing by blocking ARP responses from non-trusted sources.



Set a static mac address

```
(config)# mac-address-table static 0004.5600.67ab vlan1 int fa0/2
```

Show the mac table:

```
#show mac-address-table
```

Configure port security

```
(config)#interface fastethernet0/1
(config-if)#switchport mode access
(config-if)#switchport port-security
(config-if)#switchport port-security max 1
(config-if)#switchport port-security violation (protect/rest/shutdown)
```

BPDU guard shuts ports down when a BPDU is detected.

```
(config)#spanning-tree portfast bpduguard to apply bpduguard globally
(config-if)#spanning-tree bpduguard enable to apply bpduguard on a port
```

BPDU filter - when port is turn on, BPDU Filter sends out 10 BPDUs. If a BPDU is received then portfast is removed.

```
(config)#spanning-tree portfast bpdudfilter default to apply bpdudfilter globally
(config-if)#spanning-tree bpdudfilter enable to apply bpduguard on a port
```

Root Guard moves a port into root-inconsistent when a superior BPDU is received.

```
(config-if)#spanning-tree guard root
```

Verify inconsistent ports with the **#show spanning-tree inconsistentports**

UplinkFast

If a forwarding Port fails then the blocked port immediately transitions to forwarding. MAC addresses are then flooded out the new forwarding port

```
(config)#spanning-tree uplinkfast
```

Limit the rate that MAC addresses are then flooded out the new forwarding port

```
(config)# spanning-tree uplinkfast max-update-rate max_update_rate
```



BackboneFast

Resolves indirect link failures at twice the forwarding delay.

(config)#spanning-tree backbonefast

Duplex Mismatch

If one end is in half-duplex and the other end is set to full-duplex then it is possible that the forwarding port will not receive BPDUs for the max time period causing a blocked port on the switch to transition to forwarding mode. The switch that is in forwarding will likely NOT transition to blocked because spanning-tree does not believe that the port has a path to the root. Since both ports have a path to root a loop exists.

Duplex mismatch can be avoided with the **Loop Guard** command.

(config-if)#spanning-tree guard loop

Unidirectional Link Detection protects against Layer 1 (mis-cabling).

(config)#udld enable – turns on udld globally

(config-if)#udld enable – turns on udld on a port by port basis

#show udld interface – displays interfaces which have udld applied

