Study guide by ExamNotes.net

Exam 640-504

BCMSN

Abstract

This ExamNotes Study Guide intends to provide you with information to prepare for the Cisco 640-504 Exam.

Before you start

This study guide provides you with information on the many different aspects of "Building scalable Cisco Network". Before you proceed with this subject, please read through the study material for the following and make sure you are 100% comfortable with the Routing technology:

- CCNA 1.0 and 2.0

You need the basic knowledge about Cisco Router as well as concepts of routing. It would be nice for you to have real experience with IOS. Use Router Simulator if you do not have access to real routers:

www.routersim.com

According to Cisco's published objective at http://www.cisco.com/warp/public/10/wwtraining/cust/classes/C-TRNW-BCMSNe.html, candidates should have the following prerequisite skills and knowledge:

- Basic router configuration
- Basic switch configuration
- Basic VLAN configuration
- Spanning Tree Protocol configuration
- Inter-Switch Link configuration
- Standard access list configuration

In addition, it is suggested that students possess certain prerequisite skills using Cisco equipment, including:

- Working knowledge of the OSI reference model and the hierarchical model
- Understanding internetworking fundamentals
- Operating and configuring a Cisco IOS device
- Working knowledge of the TCP/IP stack and how to configure a routed protocol such as IP
- Understanding distance vector routing protocol operation and configuring RIP and IGRP
- Determining when to use static and default routes and enabling them on a Cisco router
- Displaying and interpreting a Cisco router routing table
- Enabling a WAN serial connection
- Configuring an IP standard and extended access list
- Verifying router configurations with available tools like show and debug commands

This study guide was written with Cisco's official documentation as the primary source of information. Do NOT rely solely on this study notes for the exam. By all means read more than one book on the subject and make sure you understand the material well enough so that you could be ready for the questions. There is no quick way to succeed for this topic. Ideally you must work things out and gain experience before even trying to sign up for the exam.

Another important thing to note is that this study guide was not written with the IOS commands in mind, as you can find much better coverage of all related IOS commands from Cisco's web site directly.

Your Study Track for BCMSN

1, Make sure you are comfortable with TCP/IP. There are many tutorials for TCP/IP on the net, and additionally you are encouraged to visit 3com's tutorial on IP addressing at: http://www.3com.com/nsc/501302.html.

For information on the OSI model, visit
http://www.rad.com/networks/1994/osi/intro.htm

2, Make sure you know the basic concept of Router configuration, Routing Protocol and IOS.

The following links include tutorial on routing protocols:

http://www.nas.nasa.gov/Groups/LAN/ClassNotes/routing/allison/

http://www.nas.nasa.gov/Groups/LAN/ClassNotes/routing/cgw_greg/

http://www.rad.com/networks/1995/ospf/ospf.htm

Additional Suggested Readings from bookstore to build up your background in routing knowledge:

- Internet Routing Architectures -- Sam Halabi, Danny McPherson(Contributor); Hardcover
- Internet Routing Architectures -- Bassam Halabi; Hardcover

3, Know about advanced switching technologies, VLAN, Unicast and Multicast:

- **802.3Ac-1998 IEEE Standard Supplement to IEEE Std 802.3-1998 : Frame** Extension for Virtual Bridged Local Area Network (Vlan) Tagging on 802.3 networks
  http://www.amazon.com/exec/obidos/ASIN/0738114219/o/qid=975933801/sr=8-1/ref=aps_sr_b_1_3/102-8154255-9855304

- Developing IP Multicast Networks: The Definitive Guide to Designing and Deploying CISCO IP Multi- cast Networks -- Beau Williamson; Hardcover
- Multicast Communication: Protocols, Programming, and Applications -- Ralph Wittmann, Martina Zitterbart; Hardcover
- Multicast Networking & Applications -- C. Kenneth Miller; Hardcover

4, Know the 504 specific topics. According to Cisco (check here), topics covered will include:

- Overview of a Campus Network
- Building a Campus Network
- Defining Common Workgroups

- Managing Redundant Links
- InterVLAN Routing
- Managing Network Traffic
- Configuring HSRP for a Fault-Tolerant Routing
- Multicast Overview
- Configuring IP Multicast

You may also find books on 504 from Amazon:

- Cisco CCNP Preparation Library, Second Edition (Cisco Career Certifications) -- Diane Teare, et al; Paperback
- CCNP: Switching Study Guide -- Todd Lammle, Todd Lammine; Hardcover
- CCNP Switching Exam Cram -- Richard Deal; Paperback
- **BCMSN: Building Cisco Multilayer Switching Networks, Course Companion (with CD-ROM)**
  by Thomas M. Thomas II, et al. Hardcover (January 15, 2000)

Traffic Flow and Switching

Options to address the broadcast containment issue for switch LAN include Creating multiple subnets and Implementing virtual LANs VLANs. VLAN represents a broadcast domain contained by a particular set of ports on switches, and that routers are required to move traffic between them. This way, VLANs segment user traffic and span multiple switches. Although routers are capable of providing packet filtering and giving wide-area access, at the expense of processing delays that limit throughput and introduces higher latency, caused by CPU overload.

The original 80/20 rule states that 80 percent of the traffic on a network segment should be local, and that no more than 20 percent of the network traffic should be able to move across a backbone. This effectively avoids Backbone congestion. The new 20/80 rule is the exact opposite. Given nowadays popularity in web-based computing and the move toward server consolidation, 20/80 is our main concern now. And this requires an improvement in Layer 3 performance.

Layer 2 switches have the ability to increase bandwidth without adding complexity as no modification is required to the packet infrastructure content. In contrast, Layer 3

routing is complex and is consuming a lot of CPU power. Layer 4 switching can make forwarding decisions based on Layer 4 parameters, traffic management, and quality of service. Multi-layer Switching is the combination of Layer 2 switching with Layer 3 protocol routing and Layer 4 parameters. The most common type of non layer 2 switching is running at layer 3, with the following advantages: Hardware-based packet forwarding, High-performance packet switching, Scalability, Low latency, Low per-port cost, Flow accounting, Security and Quality of service.

Traditional routers use general purpose CPUs, while ASICs uses high-speed hardware implementation to achieve efficient routing. This is the layer 3 switch implementation we need to suit the 20/80 needs – it integrates Layer 2 and Layer 3 functionality in a single piece of equipment.

An example of a typical multi-layer switch is the Catalyst 5000 series switch equipped with a Route Switch Module RSM or Route Switch Feature Card RSFC. The Catalyst 6000/6500 series switches equipped with a Multilayer Switch Module MSM are the common choices as well.

You may use a router together with a switch to implement multilayer switching by deploying the Netflow Feature Card on a Catalyst 5000 series switch, given the assumption that the router is directly attached to the Catalyst switch either by multiple Ethernet connections or by a Fast Ethernet connection using ISL.

To support multi-layer switching, you will need to have the following:

Multilayer Switching Switch Engine (MLS-SE)

Multilayer Switching Route Processor (MLS-RP)

Multilayer Switching Protocol (MLSP)

Commands that will be used to configure an internal or external Multi-layer Switch Route Processor include:

mls rp ip – for enabling MLSP

interface – for entering into the router interface

mls rp vlan-id – for assigning VLAN ID to route processor interface

mls rp vtp-domain – for placing an external route processor in the interface of the VTP domain switch

mls rp management-interface – for enabling the RSM interface

In contrast, to disable MLS, you will need to use the following commands: no ip routing, ip security, ip tcp compression-connections, ip tcp header-compression, clear ip-route

You use the **set mls agingtime** command to adjust the aging time. The default value is 256 seconds, and it determines when to delete an MLS entry from the cache if a corresponding flow has not been detected.

To learn how to configure MLS, please visit the following links:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_2/layer3/mls.htm

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_2/layer3/ipx_mls.htm

To learn how to troubleshoot MLS, please visit:

http://www.cisco.com/warp/public/473/13.html

For detailed information on implementing MLS, please visit:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_4_1/netflow/02pspg.htm

Campus Network

In a campus network, we deploy a hierarchical model that has 3 layers:

- Access - provide access for end users into the network
- Distribution - packet filtering, access lists, interVLAN routing, Cisco Group Management Protocol, broadcast or multicast domain definition, address or area aggregation. Always remember that the total load at the distribution layer is the number of switches at the access layer times 96Mbps.
- Core – the backbone. Subnets terminate at the core layer. With Layer 2 backbone scaling the Spanning-Tree Protocol is the bottleneck. With Layer 3 backbone scaling we can achieve fast convergence, automatic load balancing, and eliminate peering problems.

The core block is one of the key element of an internetwork. It is responsible for transferring cross-campus traffic without routing. A dual core is a core block setup that provides two equal cost paths and twice the bandwidth.

Regarding the network media used, the most common choices are Ethernet 10BaseT, Fast Ethernet, and Gigabit Ethernet. 10BaseT Ethernet allows for network segmentation at the access layer, and Fast Ethernet uses a new physical layer to run at 100 Mbs, although it uses the same frame types, length, and formats found in

10BaseT. When the network model supports dual links between each distribution layer router and core switch, 100BaseT can be deployed as the link between the access- and distribution-layer devices for aggregating traffic from each Ethernet segment on the access link. Auto-negotiation further increases network performance by allowing devices to automatically exchange link capability information. The even faster next generation of Ethernet - Gigabit Ethernet – runs at 1000Mbps and is suited for connecting access and distribution switches, connecting distribution and core switches, as well as connecting high performance servers to core switches.

VLAN

If you are planning to configure VTP and VLANs, first determine the version number of the VTP to run in your environment and decide if the switch is to be a member of an existing management domain or if a new domain should be created. The guideline to deal with this decision is that, if a management domain exist, plan for the domain name and password. You would also need to choose a VTP mode for the switch, as there are three for you to choose from. Server mode is used when this is the first Catalyst switch in your management domain, and that you will add additional switches. Client mode is used when there are other Catalyst switches in the domain. Transparent mode is used when the switch is not going to share VLAN information with any other switch on the network.

Factors you need to consider when planning the number of VLANs in a switch block include:

- group commonality
- IP addressing scheme
- traffic patterns
- types of applications
- network management

The commands you will be using to configure VLAN and VLAN trunking on a switch include **set vlan, set trunk, show trunk and clear trunk**. This reflects the correct sequence of building up a VLAN:

1. Create VLAN.
2. Assign ports.
3. Configure ports for trunking.
4. Verify configuration.
5. Remove the trunk when the trunk is no longer needed.

By definition, VLAN is a logical segment made up of defined members. Membership is mostly based on the switch port number, although it can also be based on Media Access Control addresses in some circumstances. One thing for sure is that all VLAN devices are members of the same broadcast domain, and the purpose of using VLANs is to establish broadcast domains to enjoy efficient bandwidth utilization, higher security, load-balancing multiple paths and isolation of problem components.

In an End-to-End VLAN, users are grouped independent of physical location with the same 80/20 traffic flow patterns. In a Local VLAN or a geographic VLAN, assignment is based on physical location, which can make the management process much easier and facilitate the new 20/80 rule.

VLAN membership of a user always remains the same even when he/she is moved to another location. The membership can be static (ports are manually assigned to a VLAN) or dynamic, and is based on Port through port-to-VLAN association. With ASIC, the performance of this association is very high, and is more desirable than the complex routing table lookup type of operation.

Regarding trucking, remember that an access link is a member of only one VLAN, while a trunk link is for carrying multiple VLANs in one. Dynamic Trunking Protocol is for supporting auto-negotiation of ISL / IEEE 802.1Q trunks and is for managing trunk negotiation in Catalyst supervisor engine software R 4.2 or later. Inter-Switch Link ISL is a Cisco only encapsulation protocol for interconnecting multiple switches, while IEEE 802.1Q is a method for identifying VLANs through inserting VLAN identifier into the frame header, often being referred to as frame tagging.

We use VTP VLAN Trunk Protocol for maintaining VLAN configuration consistency throughout the network. With VTP, a switch can only reside in one domain, and is listening to VTP advertisements from their own domain only. Types of advertisement include Advertisement requests from clients, Summary advertisements and Subset advertisements. Within each advertisement, you will find the VLAN Ids, the Emulated LAN names for ATM LANE, the 802.10 SAID values for FDDI, the VTP domain name, the VTP configuration revision number, the MTU size and the Frame format.

The configuration revision number is for identifying changes to the network topology. To update a switch, the configuration revision database is incremented every time a VLAN is modified. When a switch finds an advertisement with a higher configuration revision number it will save the new VTP database over the old one. A VLAN that does not exist in the new database is automatically deleted from the switch.

To add a switch to an existing VTP domain, you use the “clear config all” command to get rid of the existing configuration, then power cycle the switch, clear the VTP NVRAM content, decide on the VTP operation mode to use, and include the mode for

setting up VTP domain information on the switch. The three VTP operation modes as discussed earlier are

- Server
- Client
- Transparent

To configure VTP on a switch, you may need to use the following commands:

set vtp - For selecting VTP version.

set vtp domain – For determining management domain name

set vtp pruneeligible – For enabling VTP pruning.

show vtp – For verifying configuration.

show trunk – For verifying configuration.

For VTP Pruning, you will want to know that it does not prune traffic from VLANs that are pruning-ineligible. VLAN 1 is always pruning-ineligible, but VLANs 2 through 1000 are pruning-eligible by default, and that pruning takes effect within seconds after enabled, in order to prune for the entire management domain.

For interVLAN routing, you will want to pay attention to the following commands: show module, session, ip default-gateway, hostname

To configure interVLAN routing on an RSM, you need to create and configure VLANs on the switch, and then assign VLAN membership to the switch ports. You will then need to work on the interfaces for interVLAN routing on the RSM. Router commands that will be used include:

ip routing – for enabling ip routing protocol

encapsulation isl – for defining VLAN encapsulation

interface – for specifying VLAN interface

ip address – for assigning IP addresses to interface

interface Ethernet – for identifying VLAN interface on an external route processor

network – for initiating routing protocol on specific interfaces

router - for specifying ip routing protocol

For detailed VLAN config information and considerations, please visit the following links:

http://www.cisco.com/warp/public/732/Tech/vlan/

http://www.cisco.com/univercd/cc/td/doc/product/atm/atmsbus/79845.htm

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_2/config/vlans.htm

For VTP configuration, please visit:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_2/config/vtp.htm

STP

Bridging loops occur when a frame is transmitted from a device and then picked up by two switches. These 2 switches populate their respective address tables so that the frame is forwarded by both of them to the second segment repeatedly. Spanning-Tree Protocol (STP) is the ideal candidate to solve this problem. The formal defined function of STP is to prevent loops in a Layer 2 bridged environment.

When VLANs work together with STPs, you can control forwarding paths on a per subnet basis, which is flexible and is providing Layer 2 redundancy. Per-VLAN spanning tree can solve the scaling and stability problems in large network, while the common spanning tree CST can be used as a mean of reconciling STP and VLANs.

Bridge ID is made up of two components, namely the 2-byte priority which by default is the same for all switches, and the 6-byte Media Access Control address that represents the MAC address of the switch or bridge. These 2 components work together to determine who will become the root bridge. BPDUs are responsible for the election of a root switch for the spanning-tree topology and a designated switch for every segment. They can also be used to determine loop locations within a network and to provide notification of network topology changes. Finally, they can be used to remove loops by placing redundant switch ports in a backup state. BPDU timers are deployed to force the ports to wait for the correct topology information during propagation delays. Note that there are two factors involved in the root port selection. They are Path Cost (sum of all links crossed to get to the root bridge) and Port ID respectively.

As BPDU leaves a port, it applies the root port cost. Path cost = sum of all of the port costs, and that STP looks at it to decide which ports should forward and which ports should block. If in the case that the path cost is equal for multiple ports, STP will look at the port ID and select the one with the lower port ID first.

With CST, there will be fewer BPDUs to consume bandwidth, meaning less processing overhead. However, as there is only a single root bridge, you may end up having a less than optimum path for all devices.

Commands that deal with Spanning Tree are:

set spantree – For enabling Spanning Tree

set spantree root – For setting Spanning Tree Root Switch

set spantree secondary – For setting Spanning Tree Secondary Switch

set spantree portcost – For setting Spanning Tree Port Cost

set spantree portpri – For setting Spanning Tree Port Priority

Note that by using Fast EtherChannel technology, you can have parallel links to be treated by Spanning Tree as one physical link.

For configuring STP, you may want to first visit this link:

http://www.cisco.com/warp/public/473/5.html

HSRP

HSRP allows one router to automatically assume the function of the second router if the second router fails, thus providing redundancy and fault tolerant, as client machines generally cannot auto detect the functional default gateway. You will find the following operational states of an HSRP configured router: Initial, Learn, Listen, Speak, Standby, and Active.

In an HSRP group we have an active router for forwarding packets to the virtual router, a standby router for monitoring HSRP group status and take over the packet-forwarding responsibility should the active router fail. An active router is the one with highest standby priority in the group. It is responsible for responding to traffic for the virtual router – one that presents a consistently available router to users. With HSRP, interface tracking enables the priority to be automatically adjusted based on availability of the interfaces of a router, and reduces the chance of having a failed router remain as the active one.

To configure an HSRP standby interface, you use the command: standby ip. To set the interface "hellotime" and "holdtime" parameters, you use the command: standby

timers. To configure HSRP tracking you use the command: standby track. To display the standby status you use the command: show standby.

For more detailed information on HSRP, please visit the following links:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs009.htm

http://www.cisco.com/warp/public/619/3.html

Multicast

In Multicast, an application can send one copy of each packet to a group of computers, instead of sending it one by one to the many different recipients. In order to support multicast communications, you need to pay special attention to Addressing, as you will need a network-layer address for communicating with the group of receivers. In this regard, Class D addresses are reserved for multicast traffic and are allocated dynamically. You will also need a mechanism to map this address onto data-link layer multicast addresses. In addition, you need a dynamic registration mechanism for the computer to "join" a particular group. In this regard we have IGMP. The network must also be able to build packet distribution trees to route multicast packets. There are several standards available for multicast routing, including the Distance Vector Multicast Routing Protocol that will periodically flood packets to reach any new hosts that want to receive a particular group, and the Multicast Open Shortest Path First protocol that builds distribution tree for each source/group pair and compute tree for active sources sending to the group.

Formally speaking, IOS supports the following protocols for IP multicast routing: CGMP Cisco Group Management Protocol, PIM Protocol Independent Multicast, DVMRP Distance Vector Multicast Routing Protocol, and IGMP Internet Group Management Protocol.

The two main types of multicast routing protocols are dense mode and sparse mode. Dense mode routing protocol is ideal for situation where the multicast group members are densely distributed throughout the network and that bandwidth is sufficient. In this setting nearly all hosts can join the same group. In contrast, a sparse mode setting may have more than one group in the network. A significant difference among the two is that a dense mode router always assumes all other routers to be willing to forward multicast packets for a group, while a sparse mode router always has this assumption when there is an explicit request for the traffic.

Regarding PIM, Dense mode PIM floods the multimedia packet to all routers and prune routers that do not support members of that particular multicast group. Sparse mode PIM primarily relies on rendezvous point to run. Moreover, PIM neighbor with the highest IP address is elected the DR Designated Router. If no PIM

queries are received from this DR after a certain period of time, the election mechanism will run again.

To display settings regarding multicast, try the following commands: show ip pim interface, show ip mroute, show ip neighbor, and debug ip impacket. For detailed information on configuring multicast, please visit the following link:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/np1_c/1cprt1/1cmulti.htm

For a list of multicast IOS command, visit:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/np1_r/1rmulti.htm

For a detailed description of PIM version 2, please visit

http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_2/pimv2.htm