

Diploma in Database Administration (990) - Oracle Solaris Network Administration

Prerequisites: Detailed knowledge of Solaris	Corequisites: A pass or higher at Diploma level.
commands and Solaris Network Administration	

Aim: The Oracle Solaris Network Administration for the Solaris Operating System course provides candidates with the knowledge and skills necessary to perform network administration tasks, such as configuration and troubleshooting of a Local Area Network (LAN). The course also provides hands-on experience with topics, such as Internet Protocol (IP) routing, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), IP version 6 (IPv6) and the Solaris IP Filter firewall. Experienced system administrators who are or will be responsible for administering Oracle on a Sun system in a networked environment that includes LANs and the Solaris Operating System (Solaris OS). In this course, candidates gain the knowledge critical to properly implement and manage important capabilities in the Oracle Solaris Operating System. The course provides System Administrators, Database Administrators, and Support Personnel with advanced configuration, maintenance, and troubleshooting skills and procedures for Oracle Solaris system. Solaris Operating System is the most efficient, secure, and reliable operating system ever built; combined with Oracle; the best and most reliable Database System; this course gives candidates direct experience with the most essential system administration tasks in the networking field.

Resources.

Supplementary Materials: Lecture notes and tutor extra reading recommendations.

Special Requirements: The course requires a combination of lectures, demonstrations, discussions, and hands-on labs

and hands-on labs.			
Intended Learning Outcomes:	Assessment Criteria:		
1. Demonstrate how configuration,	1.1 Identify network topology		
administration and basic troubleshooting a	1.2 Determine how to handle name services		
network.	1.3 Analyse how IPv4 and IPv6 addressing		
	1.4 Be able to configure daemons, files and TCP/IP services		
2. Be able to monitor a system by	2.1 Analyse TCP/IP administrative tasks		
displaying all sockets, routing table entries for the inet address family for IPv4 and inet6 address	2.2 Be able to monitor interfaces and IP addresses		
family for IPv6.	2.3 Be able to use TCP/IP monitoring tools and commands		
	2.4 Demonstrate how to display Statistics by Protocol		
	2.5 Demonstrate how to display the Status of Sockets		
	2.6 Demonstrate how to display Network Interface Status		
	2.7 Demonstrate how to Display the Status of Transmissions for Packets of a Specific Address Type		
3. Describe how to configure IP tunnels and	3.1 Define IP tunnelling		
explore the history of IP Tunnels.	3.2 Be able to create tunnels		
	3.3 Be able to configure IP tunnelling		
	3.4 Describe how you manually configure IP in IP tunnels.		

4. Demonstrate how Dynamic Host Configuration Protocol (DHCP) server computers centrally manage IP addresses, other related configuration parameters and outline how DHCP client computers request IP addresses. 4.1 Explain the DHCP concepts 4.2 Describe advantages and disadvantages of using DHCP client computers request IP addresses. 4.2 Explore how DHCP server works 4.3 Explore how DHCP services 4.5 Explore DHCP Manager tasks and utilities 4.6 Be able to enable, disable, configure and administer DHCP client 4.7 Be able to troubleshoot DHCP server and client problems 4.8 Analyse files associated with DHCP 4.9 Describe the two primary differences between DHCP and BOOTP 5. Outline the Network IP Security (IPSec) architecture and be able to demonstrate IP 5.2 Outline UPSec Support Components and IPSec Core Protocols. 6. Describe how a network monitoring system help administrators to identify, climinate and prevent malfunction of hardware and software before end users encounter the problem. 6. Describe how a network monitoring system help administrators to identify, climinate and prevent malfunction of hardware and software before end users encounter the problem. 6. Describe how a network monitoring system help administrators to identify, climinate and prevent malfunction of hardware and software before end users encounter the problem. 6. Describe how a network monitoring system help administrators to identify, climinate and prevent malfunction of hardware and software before end users encounter the problem. 6. Describe how a network monitoring system help administrators to identify, climinate and prevent malfunction of hardware and software before end users encounter the problem. 6. Describe how a network monitoring system help administrators to identify, climinate and prevent malfunction of hardware and software before end users encounter the problem. 6. Describe load balancing capabilities and algorithms 6.2 Describe load balancing features 6.3 Be able to configure VRRP 6.6 Explore network congestion			
4. Demonstrate how Dynamic Host Configuration Protocol (DHCP) server computers centrally manage IP addresses, other related configuration parameters and outline how DHCP client computers request IP addresses. 4.1 Explain the DHCP concepts 4.2 Describe advantages and disadvantages of using DHCP service works 4.3 Explore how DHCP server works 4.4 Be able to configure DHCP services 4.5 Explore DHCP Manager tasks and utilities 4.6 Be able to enable, disable, configure and administer DHCP client 4.7 Be able to troubleshoot DHCP server and client problems 4.8 Analyse files associated with DHCP 4.9 Describe the two primary differences between DHCP and BOOTP 5. Outline the Network IP Security (IPSec) architecture and be able to demonstrate IP 5.2 Security Protocol Suite, IPSec Support Components and IPSec Core Protocols. 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6. Describe how a network monitoring solution of hardware and software before end users encounter the problem. 6. Describe how a network monitoring seable to create and edit IP filtering configuration files 6. Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to cinique VRRP 6.6 Explore network congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7. Describe flow accounting and statistical		3.5	•
4. Demonstrate how Dynamic Host Configuration Protocol (DHCP) server computers centrally manage IP addresses, other related configuration parameters and outline how DHCP client computers request IP addresses. 4.3 Explore how DHCP server works Be able to configure DHCP services Explore DHCP Manager tasks and utilities 4.6 Be able to enable, disable, configure and administer DHCP client 4.7 Be able to troubleshoot DHCP server and client problems 4.8 Analyse files associated with DHCP 4.9 Describe two primary differences between DHCP and BOOTP 5. Outline the Network IP Security (IPSec) architecture and be able to demonstrate IP Security Protocol Suite, IPSec Support Components and IPSec Core Protocols. 5.1 Outline IPSec tools and components 5.2 Describe IPSec security associations Analyse procedures for implementing IPSec 5.4 Describe Internet Key Exchange (IKE) 5.5 Be able to configure IKE 5.6 Analyse IP filtering 5.7 Be able to configure IKE 5.8 Be able to configure IKE 5.9 Be able to configure IKE 5.1 Describe Internet Key Exchange (IKE) 5.2 Describe Internet Key Exchange (IKE) 5.3 Be able to configure IKE 5.4 Describe Internet Key Exchange (IKE) 5.5 Be able to configure IKE 5.6 Analyse IP filtering configuration files 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7. Describe flow accounting and statistical			*
Configuration Protocol (DHCP) server computers centrally manage IP addresses, other related configuration parameters and outline how DHCP client computers request IP addresses. 4.2 Explore how DHCP server works 4.3 Explore how DHCP server works 4.4 Be able to configure DHCP services 4.5 Explore DHCP Manager tasks and utilities 4.6 Be able to roubleshoot DHCP server and administer DHCP client 4.7 Be able to troubleshoot DHCP server and client problems 4.8 Analyse files associated with DHCP 4.9 Describe the two primary differences between DHCP and BOOTP 5. Outline the Network IP Security (IPSec) architecture and be able to demonstrate IP 5.2 Outline IPSec Support Components and IPSec Core Protocols. 5.3 Analyse procedures for implementing IPSec 5.4 Describe Internet Key Exchange (IKE) 5.5 Be able to configure IKE 5.6 Analyse IP filtering 5.7 Be able to create and edit IP filtering configuration files 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6.1 Describe load balancing capabilities and algorithms 6.2 Describe Solaris load-balancing features 6.3 Be able to configure VRRP 6.4 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7. Describe flow accounting and statistical			
centrally manage IP addresses, other related configuration parameters and outline how DHCP client computers request IP addresses. 4.3 Explore bow DHCP server works Be able to configure DHCP services 4.5 Explore DHCP Manager tasks and utilities 4.6 Be able to enable, disable, configure and administer DHCP client 4.7 Be able to troubleshoot DHCP server and client problems 4.8 Analyse files associated with DHCP 4.9 Describe the two primary differences between DHCP and BOOTP 5.1 Outline IPSec tools and components Describe the two primary differences between DHCP and BOOTP 5.3 Analyse procedures for implementing IPSec Components and IPSec Core Protocols. 5.4 Describe IPSec security associations 5.3 Analyse procedures for implementing IPSec 5.4 Describe Internet Key Exchange (IKE) 5.5 Be able to configure IKE 5.6 Analyse IP filtering 5.7 Be able to correate and edit IP filtering configuration files 6.1 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.4 Define quality of service (Diffserv) architecture 7.3 Be able to create IPQoS configuration files 7.4 Describe Differentiated Services (Diffserv) architecture 7.5 Describe flow accounting and statistical			
configuration parameters and outline how DHCP client computers request IP addresses. 4.3 Explore how DHCP server works 4.4 Be able to configure DHCP services 4.5 Explore DHCP Manager tasks and utilities 4.6 Be able to enable, disable, configure and administre DHCP client 4.7 Be able to troubleshoot DHCP server and client problems 4.8 Analyse files associated with DHCP 4.9 Describe the two primary differences between DHCP and BOOTP 5. Outline the Network IP Security (IPSec) architecture and be able to demonstrate IP 5.2 Describe the two primary differences between DHCP and BOOTP 5. Outline IPSec Support Components and IPSec Core Protocols. 6. Describe PSec Security associations 7. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6. Describe Load balancing capabilities and algorithms 6. Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion control mechanism 7. Describe ways to give preferential treatment to certain types of IP traffic. 7. Describe Differentiated Services (Diffserv) architecture 7.1 Define quality of service (Diffserv) architecture 7.2 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files		4.2	
client computers request IP addresses. 4.4 Be able to configure DHCP services Explore DHCP Manager tasks and utilities Be able to enable, disable, configure and administer DHCP client 4.7 Be able to troubleshoot DHCP server and client problems 4.8 Analyse files associated with DHCP 4.9 Describe the two primary differences between DHCP and BOOTP 5. Outline the Network IP Security (IPSec) architecture and be able to demonstrate IP Security Protocol Suite, IPSec Support Components and IPSec Core Protocols. 5.1 Outline IPSec tools and components 5.2 Describe IPSec security associations Analyse procedures for implementing IPSec 5.4 Describe Internet Key Exchange (IKE) 5.5 Be able to configure IKE 5.6 Analyse IP filtering 5.7 Be able to create and edit IP filtering configuration files 6.1 Describe bow a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6.1 Describe Solaris load-balancing capabilities and algorithms Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Explore network congestion 6.7 Describe Differentiated Services (Diffserv) architecture 7.1 Define quality of service (Diffserv) architecture 7.2 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files Describe flow accounting and statistical			•
4.5 Explore DHCP Manager tasks and utilities 4.6 Be able to enable, disable, configure and administer DHCP client 4.7 Be able to troubleshoot DHCP server and client problems Analyse files associated with DHCP 4.9 Describe the two primary differences between DHCP and BOOTP 5. Outline the Network IP Security (IPSec) architecture and be able to demonstrate IP 5.2 Describe IPSec security associations 5.3 Analyse procedures for implementing IPSec 5.4 Describe Internet Key Exchange (IKE) 5.5 Be able to configure IKE Analyse IP filtering 5.7 Be able to create and edit IP filtering configuration files 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6.1 Describe Solaris load-balancing capabilities and algorithms algorithms 6.2 Describe Solaris load-balancing features 6.3 Be able to install and configure Integrated Load Balancer (ILB) 6.4 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Define quality of service 7.2 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files Describe Differentiated Services (Diffserv) architecture 7.4 Describe Differentiated Services (Diffserv) architecture 7.5 Describe flow accounting and statistical			
4.6 Be able to enable, disable, configure and administer DHCP client 4.7 Be able to troubleshoot DHCP server and client problems 4.8 Analyse files associated with DHCP 4.9 Describe the two primary differences between DHCP and BOOTP 5. Outline the Network IP Security (IPSec) architecture and be able to demonstrate IP 5. Outline IPSec Support Components and IPSec Core Protocols. 5.1 Outline IPSec tools and components 5.2 Describe IPSec security associations 5.3 Analyse procedures for implementing IPSec 5.4 Describe Internet Key Exchange (IKE) 5.5 Be able to configure IKE 5.6 Analyse IP filtering 5.7 Be able to create and edit IP filtering configuration files 6.1 Describe load balancing capabilities and algorithms 6.2 Describe Solaris load-balancing features 6.3 Be able to install and configure INTERP 6.4 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Define quality of service 7.2 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical	client computers request IP addresses.		
administer DHCP client Be able to troubleshoot DHCP server and client problems 4.8 Analyse files associated with DHCP 4.9 Describe the two primary differences between DHCP and BOOTP 5. Outline the Network IP Security (IPSec) architecture and be able to demonstrate IP 5. Security Protocol Suite, IPSec Support Components and IPSec Core Protocols. 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6.1 Describe load balancing capabilities and algorithms 6.2 Describe Solaris load-balancing features 6.3 Be able to create and edit IP filtering configuration files 6.4 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7. Describe flow accounting and statistical		4.5	•
client problems 4.8 Analyse files associated with DHCP 4.9 Describe the two primary differences between DHCP and BOOTP 5. Outline the Network IP Security (IPSec) architecture and be able to demonstrate IP 5.2 Describe IPSec security associations 5.2 Describe IPSec security associations 6. Describe Now a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6.1 Describe load balancing capabilities and algorithms 6.2 Describe Solaris load-balancing features 6.3 Be able to install and configure Integrated Load Balancer (ILB) 6.4 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7. Describe flow accounting and statistical		4.6	
4.9 Describe the two primary differences between DHCP and BOOTP 5. Outline the Network IP Security (IPSec) architecture and be able to demonstrate IP Security Protocol Suite, IPSec Support Components and IPSec Core Protocols. 5.1 Outline IPSec tools and components Describe IPSec security associations 5.2 Describe IPSec security associations 5.3 Analyse procedures for implementing IPSec 5.4 Describe Internet Key Exchange (IKE) 5.5 Be able to configure IKE 5.6 Analyse IP filtering 5.7 Be able to create and edit IP filtering configuration files 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6.1 Describe load balancing capabilities and algorithms 6.2 Describe Solaris load-balancing features 6.3 Be able to install and configure Integrated Load Balancer (ILB) 6.4 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Define quality of service 7.2 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical		4.7	
4.9 Describe the two primary differences between DHCP and BOOTP 5. Outline the Network IP Security (IPSec) architecture and be able to demonstrate IP Security Protocol Suite, IPSec Support Components and IPSec Core Protocols. 5.1 Outline IPSec tools and components Describe IPSec security associations 5.2 Describe IPSec security associations 6. Describe Analyse procedures for implementing IPSec 5.4 Describe Internet Key Exchange (IKE) 5.5 Be able to configure IKE 5.6 Analyse IP filtering 5.7 Be able to create and edit IP filtering configuration files 6.1 Describe load balancing capabilities and algorithms 6.2 Describe Solaris load-balancing features 6.3 Be able to install and configure Integrated Load Balancer (ILB) 6.4 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Describe flow accounting and statistical		4.8	*
architecture and be able to demonstrate IP Security Protocol Suite, IPSec Support Components and IPSec Core Protocols. 5.2 Describe IPSec security associations Analyse procedures for implementing IPSec 5.4 Describe Internet Key Exchange (IKE) 5.5 Be able to configure IKE 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6.1 Describe load balancing capabilities and algorithms Coescribe Solaris load-balancing features Coescribe Solaris load-balancing features Coescribe Virtual Router Redundancy Protocol (VRRP) technology Coescribe Solaris load-balancing features Coescribe Virtual Router Redundancy Protocol (VRRP) technology Coescribe Solaris load-balancing features Coescribe Virtual Router Redundancy Coescribe Virtual Router Redundancy Coescribe Solaris load-balancing features Coescribe Virtual Router Redundancy Coescribe Virtual Router Redundancy Coescribe Solaris load-balancing features Coescribe Virtual Router Redundancy Coescribe Virtual Router Redundancy Coescribe Solaris load-balancing features Coescribe Virtual Router Redundancy Protocol (VRRP) technology Coescribe Solaris load-balancing features Coescribe Virtual Router Redundancy Protocol (VRRP) technology Coescribe Solaris load-balancing features Coescribe Virtual Router Redundancy Protocol (VRRP) technology Coescribe Solaris load-balancing features Coescribe Virtual Router Redundancy Protocol (VRRP) technology Coescribe Solaris load-balancing features Coescribe Virtual Router Redundancy Protocol (VRRP) technology Coescribe Solaris load-balancing capabilities and algorithms Coescribe Solaris load-balancing capabilities and algorithms Coescribe Virtual Router Redundancy Protocol (VRRP) technology Coescribe Solaris load-balancing capabilities Coescr		4.9	
architecture and be able to demonstrate IP Security Protocol Suite, IPSec Support Components and IPSec Core Protocols. 5.2 Describe IPSec security associations Analyse procedures for implementing IPSec 5.4 Describe Internet Key Exchange (IKE) 5.5 Be able to configure IKE 5.6 Analyse IP filtering 5.7 Be able to create and edit IP filtering configuration files 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6.1 Describe load balancing capabilities and algorithms Coescribe Solaris load-balancing features Coescribe Virtual Router Redundancy Protocol (VRRP) technology Coescribe Virtual Router Redundancy Protocol (VRRP) technology Coescribe Solaris load-balancing features Coescribe Virtual Router Redundancy Coescribe Virtual Router Redundancy Coescribe Virtual Router Redundancy Protocol (VRRP) technology Coescribe Solaris load-balancing features Coescribe Virtual Router Redundancy Coescribe Virtual R	5. Outline the Network IP Security (IPSec)	5.1	Outline IPSec tools and components
Components and IPSec Core Protocols. IPSec	architecture and be able to demonstrate IP	5.2	
5.4 Describe Internet Key Exchange (IKE) 5.5 Be able to configure IKE 5.6 Analyse IP filtering 5.7 Be able to create and edit IP filtering configuration files 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6.1 Describe load balancing capabilities and algorithms 6.2 Describe Solaris load-balancing features 6.3 Be able to install and configure Integrated Load Balancer (ILB) 6.4 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Define quality of service (Diffserv) architecture 7.2 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical	•	5.3	
5.5 Be able to configure IKE 5.6 Analyse IP filtering 5.7 Be able to create and edit IP filtering configuration files 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6.1 Describe load balancing capabilities and algorithms 6.2 Describe Solaris load-balancing features 6.3 Be able to install and configure Integrated Load Balancer (ILB) 6.4 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Define quality of service (Diffserv) architecture 7.2 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical	r r	5.4	
5.6 Analyse IP filtering 5.7 Be able to create and edit IP filtering configuration files 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6.1 Describe load balancing capabilities and algorithms 6.2 Describe Solaris load-balancing features 6.3 Be able to install and configure Integrated Load Balancer (ILB) 6.4 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Define quality of service 7.2 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical		5.5	
5.7 Be able to create and edit IP filtering configuration files 6. Describe how a network monitoring system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6.1 Describe load balancing capabilities and algorithms 6.2 Describe Solaris load-balancing features 6.3 Be able to install and configure Integrated Load Balancer (ILB) 6.4 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Define quality of service 7.2 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical		5.6	
system help administrators to identify, eliminate and prevent malfunction of hardware and software before end users encounter the problem. 6.2 Describe Solaris load-balancing features Be able to install and configure Integrated Load Balancer (ILB) 6.4 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical		5.7	Be able to create and edit IP filtering
and prevent malfunction of hardware and software before end users encounter the problem. 6.2 Describe Solaris load-balancing features 6.3 Be able to install and configure Integrated Load Balancer (ILB) 6.4 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical	8	6.1	
before end users encounter the problem. 6.3 Be able to install and configure Integrated Load Balancer (ILB) 6.4 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Define quality of service 7.2 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical		6.2	•
Integrated Load Balancer (ILB) 6.4 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Define quality of service 7.2 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical			
6.4 Describe Virtual Router Redundancy Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Define quality of service 7.2 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical	before end users encounter the problem.	0.5	
Protocol (VRRP) technology 6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Define quality of service 7.2 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical		6.4	
6.5 Be able to configure VRRP 6.6 Explore network congestion 6.7 Analyse congestion control mechanism 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Define quality of service 7.2 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical		0.4	· ·
7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Define quality of service 7.2 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical		6.5	
7. Describe how IP Quality of Service (IP QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.1 Define quality of service 7.2 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical			
QoS) provide ways to give preferential treatment to certain types of IP traffic. 7.2 Describe Differentiated Services (Diffserv) architecture 7.3 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical			
to certain types of IP traffic. (Diffserv) architecture 7.3 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical			- ·
7.3 Be able to create IPQoS configuration files 7.4 Describe flow accounting and statistical		7.2	
files 7.4 Describe flow accounting and statistical	to certain types of IP traffic.		
7.4 Describe flow accounting and statistical		7.3	
		7.4	
iiii (iii iiii (iii iii iii iii iii iii			information

Recommended Learning Resources: Oracle Solaris Network Administration

1100011111	tended Learning Resources. Ordere Solding Network Hammistration
	Oracle Solaris Cluster Essentials (Solaris System Administration) by Tim Read. ISBN-10: 0132486229
Text Books	 DTrace: Dynamic Tracing in Oracle Solaris, Mac OS X and FreeBSD by Brendan Gregg, Jim Mauro, Chad Mynhier, Tariq Magdon-Ismail. ISBN-10: 0132091518 OCA Oracle Solaris 11 System Administrator Exam Guide by Paul Watters. ISBN-10: 0071775749
Study Manuals	BCE produced study packs
CD ROM	Power-point slides
Software	Solaris Operating System / Oracle Database