# Cram Guide for Exam 70-291 - Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

Created by Yu Chak Tin Michael, Sept 2004

## Implementing, Managing, and Maintaining IP Addressing

**Configure TCP/IP addressing on a server computer.**

1. Server computer should always use static IP address for itself.
2. You may configure DHCP server to use DDNS (Dynamic DNS) at the scope level or server level.
3. A scope refers to a range of IP addresses that can be issued to DHCP clients on a single subnet. You may create only one scope for each subnet, although a single DHCP server can manage multiple scopes.
4. MADCAP (Multicast Address Dynamic Client Allocation Protocol) is for issuing multicast addresses only.

**Manage DHCP.**

5. You use the DHCP snap-in to manage and monitor DHCP.
6. You may create DHCP scopes with the New Scope Wizard.

**Troubleshoot TCP/IP addressing.**

7. Most problems are the results of incorrect subnet mask or default gateway settings.
8. You may use IPCONFIG/all to verify your machine's TCP/IP information.

**Troubleshoot DHCP.**

9. You may use the /release and /renew switch of IPCONFIG to request for new dynamic IP addresses.
10. Remember to configure address exclusion on the DHCP scope if static IP is deployed on some machines.
11. For best fault tolerance, deploy multiple DHCP servers. However, watch out for conflicting scopes among these DHCP servers.

## Implementing, Managing, and Maintaining Name Resolution

**Install and configure the DNS Server service.**

12. A DNS server performs name-to-IP mapping per the request of the clients.
13. If Active Directory is installed via the Active Directory Installation Wizard, the wizard will attempt to install the DNS service for you if no existing DNS service is available.
14. Dynamic DNS is preferred in a Windows 2003 network. It is the marriage of DHCP and DNS – now you no longer need to manually update the DNS records when the IP addresses are changed.
15. MS recommends the following DNS client setting practices: If the server is the first domain controller that you installed in the domain, and the server runs DNS, configure the DNS client settings to point only to that first server's IP address. Then configure additional domain controllers that have DNS installed to point to the first domain controller that was installed in the domain and that runs DNS.

**Manage DNS.**

16. You may perform DNS management with the DNS Manager snap-in.
17. You may need to manually add resource records to the DNS database. This may be required for certain types of computer that do not support DDNS (such as the older Unix computers).
18. Active Directory Integrated DNS zone allows DNS resource records to be stored within the directory mechanism and automates the zone replication process.

**Monitor DNS.**

19. You may monitor the DNS function via Performance tool counters such as Caching Memory, IXFR Counters, TCP/IP, and Zone Transfer.
20. You may use NSlookup to examines entries in the DNS database pertaining to a particular host or domain.
21. For load balancing purpose, consider mechanisms such as Round Robin which rotates type A resource records among servers.
22. To speed up client query performance, consider to deploy cached queries through caching-only DNS servers.

## Implementing, Managing, and Maintaining Network Security

**Implement secure network administration procedures.**

23. Procedure-wise, always require authentication and secure (encrypted) connections.
24. You may secure Terminal Services communications by configuring the Terminal server to demand for varying degrees of encryption.
25. IPSec negotiates secure connection through the use of DES (Data Encryption Standard/ 56-bit) and 3DES (Triple DES) for securing packets between two hosts.
26. You use the IP Security Policy Management MMC console to manage IPSec and create policies. Do note that only one IPSec policy can be in use at a time.
27. You use IPSec filters to control when IPSec is applied.

**Monitor network protocol security.**

28. You use IPSECMON to monitor, test and troubleshoot IPSec operations.
29. To watch how IPSec Monitor functions, you need 2 Windows Server 2003-based computers that are members of the same Windows Server 2003 domain, with one computer acting as the IPSec client and the other as the IPSec server.

**Troubleshoot network protocol security.**

30. Incompatibilities may occur on client computers that are different versions of Windows and may need you to modify specific security settings and user rights assignments accordingly.
31. To troubleshoot IPSec, you should first check the results of the phase one and the phase two exchanges by enabling Audit policy so that security events can be logged in the security log of the Event Viewer.
32. You may check the active IPSec policy and filters on your computer through "netdiag /test:ipsec /debug"

## Implementing, Managing, and Maintaining Routing and Remote Access

**Configure Routing and Remote Access user authentication.**

33. To install and configure RRAS routing, right click on the server and choose Configure and Enable Routing and Remote Access on the popup menu to start the RRAS Setup Wizard.
34. Available types of remote access permissions for users include Allow access, Deny access and Control access through Remote Access Policy.

**Manage remote access.**

35. You use remote access policy to define actions that can be undertaken for a user or group who connect remotely.
36. In a Windows Server 2003-based native-mode domain, you can use the following three remote access policies: Explicit allow, Explicit deny and Implicit deny.
37. You are encouraged to use IAS (Internet Authentication Service) to centrally enforce remote access policies.
38. Remote Access Dial-in Profiles allow you to define Dial-in Constraints, IP Address Assignment Policy, Multilink, Authentication and Encryption

**Manage TCP/IP routing.**

39. To configure Windows Server 2003 as a router for a LAN, you must enable LAN routing.
40. Static routing involves manually configuring the routing table through the use of the route command in the command prompt.
41. Dynamic routing involves the use of routing protocols such as Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). RIP is the most popular routing protocol for small to mid size Windows based network.

**Implement secure access between private networks.**

42. When you start the Routing and Remote Access service Setup Wizard, you can configure one of the following options: Remote access (dial-up or VPN), Network address translation (NAT), Virtual Private Network (VPN) access and NAT, Secure connection between two private networks, Custom configuration.
43. Secure connection between two private networks is implemented through VPN tunneling.
44. Connection to the Internet should use dedicated line. WAN adapters on both sides should be configured with the IP

© Copyright 2004 CertTalk.com/Adaptive Learning Systems, Inc. All Rights Reserved.

address and subnet mask assigned by an ISP and be configured as the default gateway of the ISP router.

**Troubleshoot user access to remote access services.**

45. To monitor the activities of Routing and Remote Access and dial-up networking components, you should consider to use the tracing functionality to configure Routing and Remote Access and dial-up-networking components to log tracing information to a file. To do so, either edit the registry or use the netsh command.
46. Always remember, a dial-up connection requires both the server and the client computer to have a correctly configured modem.

**Troubleshoot Routing and Remote Access routing.**

47. Use the "route print" command to display the routing table.
48. Use the "route change" or "route delete" command to manage the existing routing entries.
49. On a WAN, communication over some routes may fail if intermediate network segments have packet sizes smaller than the communicating hosts, and black hole routers do not send appropriate ICMP responses to this condition. You use PING to identify these black hole routers.

## Maintaining a Network Infrastructure

**Monitor network traffic.**

50. You may use Network Monitor to capture and analyze network packets.
51. Capturing network activities can slow down network performance during peak hours.
52. Capture file has a default location known as the My Captures folder.

**Troubleshoot connectivity to the Internet.**

53. Portqry.exe is a command-line utility for troubleshooting TCP/IP connectivity issues. It reports the status of a TCP/IP port in one of the following three ways: Listening, Not Listening, and Filtered.
54. You may download and use DNSLint to diagnose common DNS name resolution issues.
55. You may use Tracert to verify the route used from the local host to the remote host.

**Troubleshoot server services.**

56. You may troubleshoot server services through examining the Event logs. The Event Log Service records events to the Application, Security, and System logs.
57. Certain events are written to the Directory Service and File Replication Service logs on domain controllers and to the DNS server log on DNS servers.
58. Information displayed by the Event Viewer utility includes the event type, the date and time that the event occurred, the source of the event, the category for the event, the Event ID, the user who was logged on when the event occurred, and the computer on which the event occurred.

© Copyright 2004 CertTalk.com/Adaptive Learning Systems, Inc. All Rights Reserved.