Study guide by ExamNotes.net

Exam 70-221

Designing a Microsoft® Windows® 2000 Network Infrastructure

Abstract

This ExamNotes Study Guide intends to provide you with information to prepare for the Microsoft W2K 70-221 Exam.

ExamNotes Study Guide Topics Covered

- CIDR
- QOS
- Traffic Optimization
- Security
- Availability
- NAT and ICS
- Routing
- VPN
- RADIUS
- Network Management

Before you start

This study guide provides you with information on the many different aspects of "W2K Network Infrastructure Design". You should not use this information as your first step into W2K, as this exam is targeted towards candidates with solid background on Networking.

Before you proceed with this subject, please read through the study material for the following:

- Networking Essentials
- TCP/IP 4.0
- Proxy Server 2.0
- 70-215
- 70-216
- 70-217

Topics like DHCP, DNS, WINS and RRAS are seriously overlapped!!!

Believe it or not, if you have experience on Cisco CCNA, it would help you a lot in terms of understanding the process and protocols involved in Routing.

You should setup two machines as W2K DCs and one W2K client for experimenting with DNS, DHCP, WINS and Routing on both the server and client end. To have better picture on routing and filtering, one of your server should have at least 2 NICs installed.

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 scenario questions. There is no quick way to succeed for this topic. The exam has a lot of scenario questions. You must fully understand all the related concepts and be able to think intelligently to decide what is correct and what is not. This study note can only provide you with a certain degree for assistance in preparation. You must work things out and gain experience before even trying to sign up for the exam.

Network Deployment cycle

Design:

This step involves understanding of existing network infrastructure and organizational goals. You choose which services to implement and how to combine them for maximum performance. It is also important to decide on the network management strategy at this stage.

Goals could be based on:

- Functionality
- Security
- Availability
- Performance

Implement:

You implement your network design only when it has been tested. Network monitoring is setup to collect data on its real performance.

Manage:

Maintenance of the network.

Infrastructure building blocks that you should fully understand before studying this subject:

- TCP/IP
- DNS
- DHCP
- WINS
- Proxy Server 2.0
- Remote Access

Infrastructure building blocks that needs extra study efforts:

- CIDR
- QOS
- Traffic Optimization
- Security
- Availability
- NAT and ICS
- Routing
- VPN
- RADIUS
- Network Management

CIDR

The traditional sub netting method we learned is subject to many limitations. It is advised that you analyze the network bandwidth, and if the current subnets are congested, consider to increase the number of subnets. At the same time you want to make sure that it can accommodate the number of hosts desired in each subnet. Allowing room for future growth is always the key. Also, since domain controllers in the same subnet are automatically made part of the same site in W2K, you must consider how your subnets will affect Active Directory replication when moving DCs around.

Short for Classless Inter-Domain Routing, CIDR is a new IP addressing scheme that replaces the older system based on classes A, B, and C. A CIDR IP address looks like a normal IP address except that it ends with a slash followed by a number, called the IP prefix.

172.200.0.0/16

The IP prefix specifies how many addresses are covered by the CIDR address, with lower numbers covering more addresses. For example, an IP prefix of /12 can be used to address 4,096 former Class C addresses.

We originally called CIDR as Supernetting. Under supernetting, the classed subnet masks are made classless, and we treat all classes of the addresses being combined into a subnet as Class A.

CIDR has 3 primary advantages

- reduce the size of routing tables
- make more IP addresses available
- flexibility in subnetting

Also new in W2K TCP/IP is the Automatic Private IP Addressing (APIPA) scheme used for TCP/IP address configuration for hosts on a single subnet without a DHCP server. IP addresses are allocated from 169.254.x.x/16 as specified by IANA automatically to hosts without proper IP addresses.

QOS

Short for Quality of Service, it is a networking term that specifies a guaranteed throughput level. This means to guarantee to their customers that end-to-end latency will not exceed a specified level.

Traffic control services in Windows 2000 are used to manage traffic flow for QoS-aware and non QoS-aware programs. Non QoS-aware programs uses the traffic control API (TCI) with a best effort treatment, while QoS-aware program uses the GQoS (Generic QoS API) with bandwidth reservation.

Traffic Control Components include:

- Packet Scheduler – for traffic policing
- Packet Classifier – for mapping each incoming packet to a specific priority level
- Admission Control – for deciding whether a flow can be granted without disrupting any established flows
- Resource Reservation – for setting up a flow state between end computers and inter-network devices

Queuing Methods include:

- First-In First-Out - the default mechanism used on routers that deploys store and forward method

- Priority Queuing - traffic is queued as high, normal, medium, or low, with all high-priority traffic being serviced first
- Weighted Fair Queuing - gives low-volume traffic flows preferential treatment and allows higher-volume traffic flows to obtain equity in the remaining capacity

Performance Optimization

You really have to know the nature of your network utilization in order to determine an optimal setting. Another area of concern is redundancy. Authentication, logon and encryption traffic are latency sensitive, meaning you may want to place corresponding services on both sides of a link to prevent possible disruption.

TCP/IP can be tweaked if necessary. For example, you may increase the Receive Windows Size through a registry modification to help alleviate problems with delay. TCP receive window size is the amount of receive data in bytes that can be buffered at one time on a connection. The sending host can send only that amount of data before waiting for an acknowledgment and window update from the receiving host. To change the receive window size, edit the TcpWindowSize registry parameter.

Packet loss is usually the result of router congestion. Routing updates can be the cause of high router utilization. You may combine IP ranges by supernetting to reduce routing cost. Again, even for WAN link, you need redundancy. You mat use a dial on demand interface for fall back. Higher cost metrics should be assigned to these links, as you only want them to function when the primary link fails.

Replication traffic is a major source of network slowdown. Always remember, replication based on changes increase bandwidth usage, while time based replication may not be able to update information on time. There is always a tradeoff. If yopu encrypt the replication traffic, security is achieved at the expense of high CPU utilization. Bandwidth usage is not affected much by encryption.

Static methods of name resolution, route determination and address assignment is always faster, but cannot scale well. Again, there is always a tradeoff.

As a rule of thumb, always aim for persistent high-speed connections between replication partners. This could be expensive, but this avoids a lot of headache on the way.

Sometimes it may be desirable to combine services in order to reduce the number of computers needed. This can result in cost savings as well as reduced management overhead. However, do make sure that your hardware is strong enough to handle couple services at the same time. Some services may be competing with the others for resources, which would not be suitable candidates for combination.

Security

Short for Internet Protocol security, IPSec is designed to encrypt data as it travels between two computers, protecting the data from modification and interpretation if anyone were to see it on the network. Encryption does not prevent someone to see the content, but what they see will be something totally scrambled. In W2K, administrators can monitor traffic, examine addresses, and apply various security methods to the IP data packet regardless of which program generates the data.

Using IP filtering, IPSec examines all IP packets for addresses, ports, and transport protocols. We achieve this through defining rules contained in local or group policies to tell IP Security to ignore or secure specific packets. What to filter is depending on addressing and protocol information.

The six main components of IP Security are:

- Driver - monitors, filters, and secures traffic.
- Internet Security Association Key Management Protocol (ISAKMP/Oakley) key exchange and management services - oversee security negotiations between hosts, as well as to provide keys for use with security algorithms.
- Policy Agent - looks for policies and delivers them to the IPSec driver and ISAKMP.
- Security Associations - define the security environment in which two hosts communicate.
- Security Association API - interface between the IPSec driver, ISAKMP, and the Policy Agent.
- Management tools - create policies, monitor IP Security statistics, and log IP Security events.

Encrypting data packets requires a Security Association between the two computers involved. This is the administrator's job to first define how the two computers will trust each other, and then specify how the computers will secure their traffic.

Security Association Configuration is contained in an IPSec policy that the administrator creates and applies on the local computer or using Group Policy in Active Directory.

There are two security methods that can be used by the driver separately or in unison. They are Data and address integrity through keyed hashing (HMAC) and Data integrity plus confidentiality through encryption.

IPSec Encryption Algorithms include 3DES 128-bit, DES 56-bit and DES 40-bit. IPSec Authentication Protocols include MD5 128 bit message digest 5 and SHA 160 bit secure hash algorithm. Diffie-Hellman Groups include Group One 768 bits and Group Two 1024 bits. The higher the bits number the more secure it is (and more CPU intensive too!)

IPSec Key Exchange can be achieved with:

- Preshared Keys – Uses a secret key that has been previously agreed upon by two users. The recommended method over Public Key Certificate.
- Public Key Certificates – For computers not running Kerberos v5.

Kerberos v5 is the default authentication protocol in Windows 2000 trusted domain.

Regarding DNS security, keep in mind that secured updates are only available with AD integrated zones. You want to use them to prevent impersonation of servers when using DDNS. Generally, having a DHCP server perform DNS updates is more secure, and can also reduces the headache of managing permissions. Of course, you may even encrypt replication data using VPN and IPSec for additional security, but at the expense of overhead.

One way to prevent hackers from hacking is to conceal the internal network IP structure. You may use two sets of DNS, one for the external and one for the internal network. In the internal network you use only private addresses. The internal DNS server serves only the internal clients, while outsiders' name queries are served by the DNS server outside the internal network.

Do NOT place a DHCP server outside of your firewall or inside a screened subnet, as valid IP address could be allocated to an unauthorized client. You should extend the lease times using the smallest possible address range to reduce the chance of an IP address being captured. For further security, manually mapping addresses to the MAC addresses of your clients.

Note that Windows 2000 provides two option classes for administrator to use to manage configuration details for DHCP clients within a particular DHCP scope. These option classes are vendor-defined and user-defined classes.

For WINS server that is placed outside a firewall or inside a screened subnet, you should use pull only replication from its partner, and that replication traffic should be encrypted with VPN tunnels or IPSec.

For Security purpose, PPTP connections can be used whenever remote users need access to resources on a private network, or whenever remote resources need to be secured on a user-level basis. The RRAS Setup Wizard creates a set of default Input and Output Filters on the external adapter of the VPN server. You may display and edit these filters by using the Routing and Remote Access snap-in of MMC.

Src addr	Src mask	Dest addr	Dest mask	Protocol	Src port	Dest port
Any	Any	Any	Any	47	Any	Any
Any	Any	Any	Any	TCP	1723	Any
Any	Any	Any	Any	TCP	Any	1723
Any	Any	Any	Any	UDP	500	500
Any	Any	Any	Any	UDP	1701	1701

Above is the default filter. To achieve greater security you can edit each of these filters to further restrict the flow of PPTP and/or L2TP/IPSec packets.

You may use RRAS IP filters on both the Internet and private network interfaces to grant or block access by IP address and protocol. This is done when you use the Configure and Enable Routing and Remote Access option. The five choices available are:

- Port filters
- Number of available Virtual Private Networking (VPN) interfaces
- Router properties (local area network (LAN) routing only and/or LAN and demand-dial routing)
- Remote Access Server

- Internet Connection Sharing (ICS) or Network Address Translation (NAT)

For router security, use IPSec Machine Certificates to provide a greater degree of security. Keep in mind that servers running IPSec can only communicate with other servers running IPSec, and that you will need a Certificate Authority that can issue machine-based certificates.

For VPN, Windows 2000 uses two main encryption protocols. MPPE (Microsoft Point-to-Point Encryption) is used with PPTP (Point-to-Point Tunneling Protocol) to support 40-bit, 56-bit, and 128-bit encryption. IPSec (IP Security Protocol) is used with L2TP (Layer 2 Tunneling Protocol) for encrypting user names, passwords, and data via DES (Data Encryption Standard/ 56-bit), and 3DES (Triple DES).

Compulsory VPN tunnels are initiated by the RAS server and do not require client support for tunneling. Voluntary connections on the contrary are initiated by the dial-up user and require support on the client end.

Availability

Availability does not necessarily means load balancing. Availability often refers to fall back or failover support.

One of the key components that needs high availability is DHCP. By using distributed scopes with multiple servers in remote locations you can increases availability in the event of a server failure. When the server on the local segment goes down, the one on the remote side can continue allocating addresses.

Microsoft Clustering Service MSCS increases availability by providing automatic failover if the primary node goes down and failback when the downed server comes back online. The two servers must be of identical setup, and must be locally connected at high speed consistently.

Before you install MSCS, verify that your hardware is on the Hardware Compatibility List as a complete cluster solution. The following information must be on hand for verification:

- Server 1: manufacturer and model number

- Server 2: manufacturer and model number
- SCSI/RAID controller: manufacturer and model
- Shared SCSI/RAID controller: manufacturer and model

To avoid the possibility of a power outage which could cause both nodes to restart at the same time, change the Boot.ini file timeout value of one node to 10 seconds and change the value of the other node to 90 seconds.

NAT and ICS

Network address translation is for hiding your real IP addresses, or for a group of computers to share internet access. Proxy server to a certain extent has NAT functions too. In most cases, it is only appropriate for non-routed network environments where all users have the same access privileges but where private addressing for all computers is required.

You may want to use NAT when you want to exchange traffic between two dissimilar network segments, or to create screened subnets. Proxy Server is an ideal candidate, but make sure you understand the complexity involved in deploying Proxy Server. By default, all computers behind NAT are inaccessible from the Internet, meaning your internal network is safe to a certain extent.

You should dedicate a system for running NAT for both performance and availability. Remember, NAT can have conflicts with DHCP, so you better separate these two services.

ICS provides networked computers with the ability to share a single connection to the Internet. Connected devices receive transparent network configuration using Directory Naming Service and Dynamic Host Configuration Protocol to resolve Internet names. All these are achieved via the following components:

- DHCP Allocator - simplified DHCP service
- DNS Proxy - resolves names on behalf of local network clients
- Network Address Translation
- Auto-dial - Automatically dials connections

- APIs - for configuration, status, and dial control for programs.

ICS is recommended mainly for small home network. For large network, ICS is not preferred. Keep in mind, ICS's DHCP and DNS components are not configurable, and may cause conflicts with your regular DHCP and DNS services.

Routing

Routing is the process of moving a packet of data from source to destination. It is usually performed by a dedicated device called a router. W2K Servers can act as routers. Each intermediary computer performs routing by passing along the message to the next computer, and part of this process involves analyzing a routing table to determine the best path. Normally a router should have 2 NICs, although W2K Server supports routing with a single NIC.

RIP Routing Information Protocol is a protocol defined by RFC 1058 that specifies how routers exchange routing table information. It supports IP and also IPX. Routers periodically exchange entire tables, which is inefficient, and is gradually being replaced by a newer protocol called Open Shortest Path First (OSPF).

Open Shortest Path First is a routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Routers use link-state algorithms to send routing information to all nodes by calculating the shortest path to each node based on a topography of the Internet constructed by each node. Since each router sends that portion of the routing table that describes the state of its own links rather than the entire table, it is more efficient than RIP. OSPF also results in quick converge time and prevent problems like routing loops and Count-to-Infinity. All these are at the expense of high CPU power and memory utilization.

With OSPF, there are three main components. OSPF Autonomous System is a collection of networks that share a common administrative authority. OSPF Area is a group of routers that are all connected by area border routers into a backbone area. OSPF Network is the smallest unit that consists of individual segments that are connected by OSPF routers.

For scalability reason, use OSPF instead of RIP. If your network is small, consider RIP as it is a much simpler mechanism. Use RIP when there are frequent changes to routing information, demand-dial interfaces are used, or there are no more than 14 hops between routers. For network using VLSM, if RIP is the choice, use RIP V2. And

most importantly, make sure all your routers in the same network speak the same language.

Short for Internet Group Management Protocol, IGMP is defined in RFC 1112 as the standard for IP multicasting in the Internet. It's for establishing host memberships in particular multicast groups on a single network. The mechanisms allow a host to inform its local router, using Host Membership Reports, that it wants to receive messages addressed to a specific multicast group. Note that all hosts conforming to level 2 of the IP multicasting specification require IGMP. In W2K, RRAS has two modes of IGMP support. Proxy Mode forwards multicast traffic to a multicast capable router, while Router Mode will listen for and update the multicast-forwarding table.

One last thing about routing. Routers placed at the edge of a network is a good candidate for providing firewall type security when packet filtering is enabled. If you are to use software based routing solution such as W2K, use a dedicated computer as a router for the best performance.

RADIUS

Short for Remote Authentication Dial-In User Service, RADIUS is an authentication and accounting system used by many Internet Service Providers. When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the system.

Internet Authentication Service IAS is Microsoft's implementation of RADIUS. RADIUS and IAS together perform centralized connection authentication, authorization, and accounting for dial-up and virtual private network connections.

In general we like to place RADIUS clients as near as possible to remote users creating a local point-of-presence to reduce administrative overhead by delegating administration to local network administrators in the same area. Also, RADIUS servers should be placed as close as possible to the server that provides authentication in order to have them in the same private network and prevent unauthorized access.

With AD integration, RADIUS server must have a high-speed persistent connection to the global catalog server. You may even install IAS on the global catalog server to increase authentication performance.

For availability, you should install redundant RADIUS clients and give remote users phone number for the primary and backups. Please make sure there are sufficient phone lines and modems to handle the user load.

For security, Microsoft recommends that you specify connections between the RADIUS client and the server to use VPN or IPSec encryption. For communication between RADIUS servers, use RADIUS secrets for authentication.

Types of W2K supported authentication protocols include PAP (Password Authentication Protocol), SPAP (Shiva Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) and MS-CHAPv2 (Version 2).

Network Management Strategies

With In-band data collection, status data traverses the same network that provides services. This traffic can impact the network if large amounts are collected. Out-of-band data collection has the status data gathered via separate network connections.

You may run scripts or batch files to read accumulated performance data provided by application logs, event logs, and performance logs. From these you may generate event notifications when certain pre-programmed thresholds are exceeded. Of course, if you have the resource, you may write custom programmed applications to manage network services as well. MMC is customizable in the form of snap-ins.

The following is a list of network management and troubleshooting tools you should play with: NBTSTAT, NETDIAG, NETSTAT, Network Monitor, NSLOOKUP, PATHPING, PING, and TRACERT. For event logs, you want to focus on the following event types: Error, Information, Warning, Success Audit, and Failure Audit.