Windows 2000 Network Infrastructure - CramNotes



Before you start

This study guide provides you with information on the many different aspects of "W2K Network Infrastructure". You should not use this information as your first step into Networking, as this exam is targeted towards candidates with real experience and solid background on Windows Networking and TCP/IP. If you are a beginner, I recommend that you first study the material presented in the NT 4.0 track Networking Essential and TCP/IP, and then complete the 210 and 215 exams before working on this one.

Due to the fact that 210, 215, 216 and 217 have many topics overlapping, we have arranged the study guides in the following manner:

210 Guide and 215 Guide will focus on the installation, hardware, file systems, resource management and other client services issues. 216 is focused on Active Directory, and 217 is focused on the infrastructure side, including DNS, DHCP, WINS and Protocols, Routing, Security...etc. To prepare for any particular exam, we recommended that you go through all of them. This will make sure you have a complete picture of a "W2K network scenario".

We are compressing 600+ pages of information into a 10-page study guide as a summary of what you need to learn. Please do not use this study guide as your only study resource. To pass a W2K exam, you need to read many different books and have real hands on experience.

Suggested Reading

Exam Cram, McSe Windows 2000 Network: Exam 70-216 (Exam Cram) by Hank Carbeck, et al. Paperback (September 28, 2000)

MCSE Windows 2000 Accelerated Study Guide (Exam 70-240) (Book/CD-ROM package) by Tom Shinder(Editor), et al. Hardcover (October 6, 2000)

MCSE 2000 JumpStart: Computer and Network Basics by Lisa Donald, et al. Paperback (April 2000)

MCSE: Windows 2000 Network Infrastructure Administration Exam Notes by John William Jenkins, et al. Paperback (September 19, 2000)

Public Key Infrastructure Essentials: A Wiley Tech Brief -- Tom Austin, et al; Paperback

<u>Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure</u> -- Russ Housley, Tim Polk: Hardcover

Digital Certificates: Applied Internet Security -- Jalal Feghhi, et al; Paperback

<u>Ipsec: The New Security Standard for the Inter- net, Intranets, and Virtual Private Networks</u> -- Naganand Doraswamy, Dan Harkins; Hardcover

A Technical Guide to Ipsec Virtual Private Networks -- Jim S. Tiller, James S. Tiller; Hardcover

Big Book of IPsec RFCs: Internet Security Architecture -- Pete Loshin(Compiler); Paperback

VPN Applications Guide: Real Solutions for Enterprise Networks -- David E. McDysan; Paperback

Protocols

TCP/IP is a suite of protocols that provide routing in WANs as well as connectivity to different hosts on the Internet. W2K supports version 4 of TCP/IP. Actually, W2K needs TCP/IP together with DNS to survive.

IP address on the internet are divided in Class A, B, C, D and E. All classfull IP address contains a self-encoding key that identifies the dividing point between the network-prefix and the host-number.

Class A Networks uses /8 Prefixes, meaning each Class A network address has an 8-bit network-prefix with the highest order bit set to 0 and a seven-bit network number, followed by a 24-bit host-number. Under Class A, a maximum of 126 (27 -2) /8 networks can be defined.

Class B Networks uses /16 Prefixes, meaning each Class B network address has a 16-bit network-prefix with the two highest order bits set to 1-0 and a 14-bit network number, followed by a 16-bit host-number. Under class B, a maximum of 16,384 (214) /16 networks can be defined with up to 65,534 (216 -2) hosts per network.

Class C Networks uses /24 Prefixes, meaning each Class C network address has a 24-bit network-prefix with the three highest order bits set to 1-1-0 and a 21-bit network number, followed by an 8-bit host-number. Under class C, a maximum of 2,097,152 (221) /24 networks can be defined with up to 254 (28 -2) hosts per network.

In addition, we have class D and E. Class D addresses have their leading four-bits set to 1-1-1-0 and for supporting IP Multicasting. Class E addresses have their leading four-bits set to 1-1-1-1 and are reserved for experimental use. To make Internet addresses easier for us to read and write, they are expressed as four decimal numbers separated by a dot. This divides the 32-bit Internet address into four 8-bit fields.

Subnetting an IP Network can be done to control network traffic, as it effectively segment the broadcast domain into smaller independent segments connected by routers. A router is used to connect IP networks to minimize the amount of traffic each segment must receive. You apply a subnet mask to an IP address to identify the network and node parts of the address:

- Class A 255.0.0.0 111111111.00000000.00000000.00000000
- Class B 255.255.0.0 111111111.11111111.000000000.00000000
- Class C 255.255.255.0 111111111.11111111.111111111.000000000

With classless subnetting, you are no longer limited to the class structure. Instead, you determine the suitable network prefix by yourself. RFC 1009 specified how a subnetted network could use more than one subnet mask, that is, when an IP network is assigned more than one subnet mask, it is considered a network with "variable length subnet masks" VLSM, as the extended-network-prefixes can have different lengths. This effectively supports more efficient use of an organization's assigned IP address space. However, for VLSM to run successfully, the following conditions must be met:

- routing protocols must carry extended-network-prefix information with each route advertisement.
- routers must implement a consistent forwarding algorithm based on the "longest match" principle.
- addresses must be assigned so that they have topological significance for route

aggregation to occur.

An internal router is a router with all interfaces connected to the same local areas, while a border router is one with interfaces connected to different outside areas. In Windows 2000, the administrative tool you use to manage internal and border routers is the Routing and Remote Access component.

To lessen the load of router, we want to make the routes as simple as possible. We do this through CIDR. CIDR stands for Classless Inter-Domain Routing. It is documented in <a href="https://recommons.org/recommon

The most common TCP/IP utilities used to verify and test a TCP/IP configuration are PING and Ipconfig. You are strongly encouraged to check out the CCNA study material available on the web. You will find information regarding the following terminology. You need to know them in order to pass this exam:

- O CIDR
- Routed Protocol
- Routing Protocol
- O RIP
- O OSPF

For more information and tutorial on routing, please visit http://www.scit.wlv.ac.uk/~jphb/comms/routing.html

You should also revisit information on NT 4's Routing related topics, such as the use of the Route command and the related troubleshooting utilities.

NWLink is the Microsoft implementation of Novell's IPX/SPX. You must use this protocol if you want to use Gateway Service for NetWare or Client Service for NetWare to connect to NetWare servers, even if you are running Netware 5. TCP/IP cannot be used to communicate with any version of Netware server.

Gateway Service for NetWare allows you to create a gateway for Microsoft client computers to access NetWare file and print resources. If you intend to create or indefinitely maintain a heterogeneous environment composed of both servers running Windows 2000 and NetWare, you should go with Client Service for Netware instead. Otherwise, if you only want to migrate gradually from NetWare to Windows 2000, or to reduce administration, stick with the gateway service.

NWLink has an Auto Detect feature that detects the frame type and network number configured on NetWare servers on the network. If in case the Auto Detect feature selects an inappropriate frame type and network number for a particular adapter, you should manually reset them for that given adapter.

Sometimes you may want to analyze frames. Network Monitor allows you to identify client-to-server connection problems, locate a computer that makes a disproportionate number of requests, and isolate Application Layer problems. A capture filter is used to specify the types of network information you want to monitor. By filtering frames, you can save buffer resources and analysis time. Note that each frame contains the source address of the sender, the destination address of the recipient, headers from each protocol used within the frame, and the

payload.

DNS, WINS and DHCP

It is impractical to identify each system solely by its numeric IP address. In contrast, names are more than a convenience as they help users and administrators locate network resources more easily. The Domain Name System DNS is a distributed database holding the alphanumeric names and IP addresses of every registered system on the Internet or intranet, depending on what this DNS server is targeted for. Resolvers are responsible for passing name requests between applications and name servers. Domains define levels of authority in a hierarchical structure, with the top of the hierarchy as the root domain. Then we have those Top-Level Domains such as .com, .net, .edu...etc. At the next level of the hierarchy are the middle-level domains that we run. We use authoritative name servers hold data for these domains. A master name server is the source of the downloads for a secondary name server which could be a primary or secondary name server. The reasons we want to set up a secondary name server are:

- o you should have at least one redundant name server for each zone
- o to avoid remote clients from communicating across slow WAN links
- o reduces the load on the primary name server

You should know the difference between a domain and a zone. A domain is a branch of the DNS name space, while a zone is a portion of a domain that has a separate file on the disk for storing resource records. Note that a single DNS server can be configured to host zero, one, or multiple zones. You have to judge based on the actual load of the DNS server. A caching-only server only caches query results. It does not generate zone transfer network traffic as it does not contain any zones. It basically builds up cache information over time as it services requests.

In W2K, DNS Server supports Dynamic update to enable DNS client computers to register and dynamically update their resource records with a DNS server automatically should changes occur. This greatly reduces the need for manual administration. For a successful Windows 2000 DNS implementation, you need to have the following three components:

- Database file
- Cache file
- Reverse lookup file

To monitor DNS performance, watch out for the following types of counter:

- O Dynamic update and secure dynamic update counters
- Memory usage counters
- Recursive lookup counters

WINS in W2K is an alternative name resolution mechanism for backward compatibility. It supports the automatic name registration and resolution of NetBIOS names and provides internetwork / interdomain browsing. In W2K, you can specify up to 12 WINS servers. You can set up pull or push replication partnerships for the WINS server. Keep in mind that pull replication is based on time, while push replication is based on data changes. Pull replication is ideal for slow WAN link, as you can specify replication to occur at midnight or at any non-office hour.

DHCP simplifies the administrative management of IP address configuration by automating address configuration for network clients. Since a DHCP server can enable dynamic updates in the DNS name space, clients can update their computer name-to-IP address mapping

information whenever changes occur to their DHCP-assigned address. A DHCP client can be any networked computer that requests and uses the DHCP services offered by a DHCP server.

Note that Windows 2000-based clients can automatically configure an IP address and subnet mask if a DHCP server is unavailable at system start time. This auto configured address will be replaced by one offer by the DHCP server when the DHCP server is back online. To manage DHCP servers in Windows 2000, we use the DHCP Manager of MMC. Keep in mind that a DHCP must be authorized in AD in order to function. For the directory authorization process to work properly, the first DHCP server introduced onto the network must participate in the Active Directory service and must be installed as either a domain controller or a member server.

Note that as DHCP requires initial broadcast, if there is a router in between, you need to install DHCP Relay Agent for DHCP to work in the subnets.

NAT and Remote Access

NAT Network Address translation allows computers on a small network to share a single Internet connection or to hide the internal IP addressing scheme. The NAT translation component is the router on which NAT is enabled. The NAT addressing component provides IP address information to other computers on the internal network. The name resolution component acts as the DNS server for the computers on the internal network.

NAT maps IP address with either static or dynamic mappings. To allow Internet users to access resources on your private network, you must use static IP address configuration on the resource server. This static address should be excluded from the range of IP addresses being allocated by the NAT computer. You will also need to configure a special port for static mapping of public address and port number to a private address and port number. Proxy Server supports similar functionality, but is more complex to implement.

W2K can support remote user connection via dial up modems or ISDN. Old concepts like multilink and call back security still apply. The test will test your knowledge on default gateway setting, so you should be able to identify the correct IP that should be placed in a particular configuration.

Security

Windows 2000 supports three authentication methods, with Kerberos V5 security as the default authentication technology. The Kerberos protocol issues tickets when a computer logs on to a trusted domain. Everything is ticket based. To use Certificates as the authentication method requires at least one trusted certificate authority to be configured. Windows 2000 supports X.509 Version 3 certificates. Preshared Key uses previously agreed key value as a way to authenticate.

IP SECurity is a security protocol from the IETF that provides authentication and encryption over the Internet. It works at layer 3 and secures everything in the network. It is a communications protocol that encrypts and decrypts a message for online transmission. Web browsers and servers generally support IPSec.

With IPSec, a public key certificate allows a nontrusted domain computer to use IPSec to communicate with a trusted domain computer. Secret key cryptography uses a single preshared key for encryption and decryption, while public key cryptography uses a key pair, with one for

encrypting data and the second one for decrypting data. We use ISAKMP/Oakley to establish secure channel between two computers for communication and establishes Security Association. For additional security, IP filters can be used to check datagrams for a match against each filter specification. Filtering can be based on the source and destination address, DNS name, protocol, or protocol ports...etc.

An IPSec policy is a collection of rules and key exchange settings assigned as a domain security policy or an individual computer's security policy. A domain computer automatically inherits the IPSec policy assigned when it logs on to the domain. If a computer is not connected, IPSec policies are in the local computer registry. Rules inside the policy are comprised of IP filters, negotiation policies, authentication methods, IP tunneling attributes, and adapter types. In general, one security policy can be created for all users on the same network or all users in a particular department. We create IPSec policies via the IPSec Management MMC snap-in.

To monitor and troubleshoot IPSec, use IP Security Monitor IPSECMON.EXE to monitor IPSec related security statistics, or use Network Monitor V2.0's parser for IPSec to capture related information transferred over a network interface at any given time. Note that if IPSec is encrypting the packets, then the actual contents will not be visible. If only authentication is used, the entire packet will be visible.

A certificate is a digital document that attests to the binding of a public key to an entity for generating confidence that the public key contained actually belongs to the entity named in the certificate. A certificate authority CA is responsible for issuing certificates. The 4 types of Microsoft certificate authorities are:

- Enterprise root CA
- Enterprise subordinate CA
- Stand-alone root CA
- O Stand-alone subordinate CA.

Put it this way, a certificate is just a file digitally signed by a signing authority. It contains two parts: the private part and the public part. Generally speaking, certificates are primarily concerned with digital signatures, although they can be used for encryption. Certificates hold your public keys so that other people can encrypt the data they send you. It is important to know that most of the time you will need passphrases for your browser and for each certificate. If you forget a passphrase, you will never be able to use the certificate again.

For more information about Public Key Infrastructure PKI, digital certificates and CAs, please visit

http://www.elsop.com/wrc/digicert.htm

http://www2.commerce.virginia.edu/dsc4y/ET/pkilinks.htm

http://www.alw.nih.gov/PKI/general-refs.html

For remote connection, we can use the Routing and Remote Access service. VPN is a simulated point-to-point connection using encapsulation. The two supported VPN protocols are L2TP and PPTP. Remote access via Demand-dial can be protected by filters that screen traffic based on the following fields of a packet:

- Source and destination IP address
- IP protocol identifier
- Source and destination ports
- ICMP type and ICMP code

In addition, you may set dial-in user permissions to Allow Access or Deny Access through the User Property page if RAPs Remote Access Policies are not used. What are RAPs? RAPs are for defining who has remote access to the network and what the characteristics of that connection will be. You specify conditions for accepting or rejecting connections based on many different criteria, including day and time, group membership, and type of service. Note that Remote Access Policies are stored locally in the IAS.MDB file of the server. Even if the user's permission is Allow Access, he/she must still meet the conditions set forth in a RAP.

To secure your organization's network if it is connected to the internet, you should put a firewall between the two networks to prevent unauthorized access to your computers from the Internet. Also note that Routing and Remote Access can use secure user authentication method for maximum protection. Methods that can be used include:

- Challenge Handshake Authentication Protocol (CHAP)
- O Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
- Password Authentication Protocol (PAP)
- O Shiva Password Authentication Protocol (SPAP)
- O Extensible Authentication Protocol (EAP)

Especially with smart card, you must use EAP.

For more information on firewall, please visit http://www.alliancedatacom.com/firewall-tutorial.htm

Event Viewer can be used to monitor Windows 2000 security events, including valid and invalid logon attempts as well as object access via the security log.

Before you register for the exam

Please make sure you go through the other W2K Study guides. Due to the fact that 210, 215, 216 and 217 have many topics overlapping, we have arranged the study guides in the following manner:

210 Guide and 215 Guide will focus on the installation, hardware, file systems, resource management and other client services issues. 216 is focused on Active Directory, and 217 is focused on the infrastructure side, including DNS, DHCP, WINS and Protocols, Routing, Security...etc. To prepare for any particular exam, we recommended that you go through all of them. This will make sure you have a complete picture of a "W2K network scenario".

This CramNotes is written by Michael Yu Chak Tin. He can be contacted by email at: ycthksuccess@ctimail3.com. Please also visit his homepage at http://michaelyu.freeservers.com/