Networking and Name Resolution: Section 1 Transcript

Introduction 1/2

Welcome to the Networking and Name Resolution module.

In this module we will be discussing standard Windows networking services and the process of Windows Name Resolution.

Throughout this module, you'll be presented with opportunities to assess and apply what you've learned.

At the end of this module, you will be able to:

- Describe common Windows networking services and ports,
- Demonstrate ability to use Windows networking commands,
- Identify common commands when using the Netstat tool,
- Demonstrate ability to map listening ports to startup location,
- Explain DNS and NetBIOS Name resolution, and
- Explain the difference between host names and NetBIOS names.

Bypass Exam Introduction 2/2

If you are already familiar with the subject matter presented in this module, you can choose to take a Bypass Exam to skip this module.

The Bypass Exam option provides a single opportunity to successfully demonstrate your competence with the material presented within the module. If you pass, you'll receive credit for completing the module, unlocking the content within, and you will be free to proceed to the next module. If you do not pass, you will need to successfully complete the module, including all exercises and the Module Exam, to receive credit.

Click the Next Section button to continue.

Networking and Name Resolution: Section 2 Transcript

Windows Networking Services

Standard Windows networking services are associated with specific ports. Remember, a port is an application-specific or process-specific software construct serving as a communications endpoint in a computer's host operating system. We will talk about two types of ports: well-known and ephemeral. Well-known ports are associated with the port numbers 1 through 1023 and are assigned to specific services. On Windows Vista and later OS's, ephemeral ports randomly assign port numbers 49152 through 65535 for services that are not defined within the well-known ports range. The ephemeral port range for Windows XP and Windows 2003 was 1025 through 5000 until the release of Service Pack 2, which expanded the range to 1025 through 65535. In this module, we will discuss a few standard Windows services: Remote Procedure Call (RPC), Server Message Block (SMB), and NetBIOS. These services use UDP, TCP, or both.

Remote Procedure Call (RPC)

Remote Procedure Call (RPC) serves as a go-between for client/server communications. It is designed to provide a common interface between applications and make client/server interaction easier and safer. RPC achieves this by factoring out common tasks such as security, synchronization, and data flow handling, into a common library. This ensures developers do not need to dedicate the time and effort into developing their own solutions.

Much of the Windows architecture is composed of services that communicate with each other to accomplish a task. Most services built into the Windows architecture use RPC to communicate with each other. For example, the Windows server domains protocols are entirely Microsoft RPC, or MSRPC, based, as is Microsoft's Domain Name System (DNS) administrative tool.

The RPC application programming interface (API) provides access to an extensive set of run-time operations according to the operations performed. These operations include:

- Binding-related operations,
- Name service operations,
- Endpoint operations,
- Security operations,
- Stub memory management operations,
- Management operations, and
- Universal Unique Identifier (UUID) operations.

End Point Mapper

The End Point Mapper is a function of the RPC service on port 135 that facilitates the RPC bind to the application. The End Point Mapper can be queried to determine an operating system type and

determine which services are using RPC.

It is used to remotely manage services including:

- DHCP,
- DNS,
- WINS, and
- DCOM

Let's talk about how this works.

End Point Mapper

When a computer's RPC services initialize, they register with the RPC End Point Mapper service (epmapper).

A client computer connects to the epmapper service on TCP port 135 and queries for a specific RPC service. If the service is not available, the client terminates the connection. Otherwise, the client sends a request to connect to the desired service.

The server responds to the connect request with the protocols to be used to connect to the RPC service.

The client has two options:

- It connects using one of the specified protocols, and the RPC operation continues, or
- It attempts to connect using a protocol that was not specified and generally results in a failed connection attempt, as they are rejected by the server.

Server Message Block (SMB) Protocol

The Server Message Block (SMB) Protocol provides a method for client applications in a computer to read and write to files on and to request services from server programs in a computer network. Using the SMB protocol, an application (or the user of an application) can access files at a remote server as well as other resources, including printers, mailslots, and named pipes. What this means is that a client application can read, create, and update files on the remote server. It can also communicate with any server program that is set up to receive an SMB client request.

The Server Message Block protocol can run on top of the Session (and lower) network layers in several ways:

- Directly over TCP, port 445;
- Via the NetBIOS API, which in turn can run on several transports to include on UDP ports 137 and 138, and TCP ports 137 and 139

Mailslots and Named Pipes

So what are these mailslots and named pipes that SMB (and other services) uses?

A mailslot is a mechanism for one-way inter-process communications. Applications can store messages in a mailslot, and the owner of the mailslot can retrieve messages that are stored there. These messages are typically sent over a network to either a specified computer or to all computers in a specified domain.

A named pipe is a bi-directional connection for communication. Named pipes can be used to provide communication between processes on the same computer or between processes on different computers across a network.

Named pipes are a simple way for two processes to exchange messages. Mailslots, on the other hand, are a simple way for a process to broadcast messages to multiple processes. One important consideration is that mailslots broadcast messages using datagrams, and there is no way to guarantee that a datagram has been received. In contrast, named pipes are like telephone calls where you only talk to one person and you know that the message is being received.

Network Basic Input/Output System (NetBIOS) 7/10

NetBIOS (Network Basic Input/Output System) allows applications to communicate over a network. It is asoftware interface defined by RFC 1001 and RFC 1002 that provides a standard API for user applications to submit network inputs and outputs and control directives to underlying network protocol software. An application program that uses the NetBIOS API for network communication can be run on any protocol software that supports the NetBIOS interface. This is possible because NetBIOS frees the application from needing to understand the details of the network. This means that the application developer does not need to make the application interact with and understand all of the lower working operations and functions of the network stack. Instead, the application can just let NetBIOS handle all of that.

It may be a good time to introduce NetBIOS over TCP/IP (NetBT). NetBT is a protocol that allows computer applications that rely on the NetBIOS API to be used over TCP/IP. NetBIOS is becoming a legacy protocol since it was originally developed for non-routable LANs. DNS (host names) has primarily taken over, and NetBT just allows compatibility for older systems still running NetBIOS.

NetBIOS 8/10

NetBIOS supports three services: NetBIOS Datagrams, NetBIOS Sessions, and NetBIOS Name Management. Let's talk about each one.

Datagram distribution service
Datagram mode is "connectionless". Since each message is sent independently, they must be smaller and the application becomes responsible for error detection and recovery. In this mode, the datagram service and mailslot run on UDP port 138.

Session service
In session mode, NetBIOS lets two computers establish a connection for a "conversation", allows larger messages to be handled, and provides error detection and recovery. In NetBIOS over TCP/IP (NetBT), the session service and named pipes run on TCP port 139.

Name management service

Computer names, user names, and domain names, to name a few, must all be resolved to ensure the right messages and shared resources can be identified and contacted for authentication. Applications must register their NetBIOS name using the name service. In NetBIOS over TCP/IP, the name service operates on UDP port 137 (TCP port 137 can also be used, but it is rarely if ever used). We will discuss name resolution in more depth later in this module.

Windows Networking

Welcome to the Windows Networking video. I'll be your guide for this video presentation.

As the systems on which we are operating are being accessed over a network, it's important to analyze the network configuration and state on every system. This will give us context about where we are operating and help develop target situational awareness.

In this presentation, we will review the tools used to view and modify network configuration and state on most Windows systems.

As you run these commands on a live system, you should always be asking yourself, "What does this information tell me about the network in which this system lives?" and "What does it tell me about the system's role in its network?"

Ok, let's get started!

Choosing ipconfig as your first command is useful in determining if this host is the host you expect it to be, generally by comparing the hostname, or sometimes the IP, if you know they statically configure them to information you already have. Using the /ALL option displays the full configuration for all network interfaces.

The netmask is a 32 bit mask that is used to divide an IP address into subnets and identify host addresses. This allows you to determine the number of possible hosts, or size, of the subnet.

The default gateway address identifies where traffic is sent that is destined for a network other than the network the sender is on.

The MAC address is the hardware address of the system.

The DNS server addresses point to the destinations where name queries are sent.

A DNS Suffix is the domain portion of a DNS address. For instance, consider: Computer1.domain.net. "Computer 1" is the hostname portion and "domain.net" is the DNS suffix. A 'suffix search list' is a list of DNS suffixes that the name resolver appends to a DNS search, in the order listed, in an attempt to resolve the search.

The "displaydns" option displays the DNS cache of the system. This includes preloaded data from the Hosts file as well as recently obtained records.

The hostname command prints the name of the local machine.

Both "route print" and "netstat -r" display the routing table. A routing table is a collection of destination networks and how to get there. They can be maintained dynamically or manually, and

serve as record for all the networks that the system knows how to reach, including the default route.

Netstat -anob is the standard netstat command that displays all active and listening connections, does not attempt to resolve names, and includes the process ID for each entry. Adding the -b option also includes the process name for each netstat entry.

Arp -a displays the arp cache for all interfaces. The arp cache is a mapping of the IP and MAC addresses of devices the system has recently had a need to talk to. Unless specifically made permanent, each entry is temporary.

All three of these command possibilities display the domain name of the system. The 'echo' command only shows the NetBIOS version of the domain name. If the system is not in a domain, the 'echo' command returns the system name.

Ipconfig /release discards the DHCP configuration on network adapters that have DHCP enabled. If a specific interface is added to the command, only that interface is affected by the command.

Ipconfig /renew re-establishes the DHCP configuration on all interfaces with DHCP enabled. Only one specific interface can be renewed if it is specified on the command line.

In the GUI, you can modify a system's IP address, Netmask, Gateway and DNS servers. This can also be accomplished in the command line.

The netsh command allows you to alter a network card's IP, subnet, and gateway address.

Though the computer name can be changed in the GUI, this can be done in the command line as well.

This wmic command renames the local systems host name to "dev_PC_06".The netsh command allows you to alter a network card's IP, subnet and gateway address.

Please note the change will not take effect until the next reboot.

A static route is a manually configured routing table entry.

By using the "-p" option, the static route will be maintained across reboots.

A static route can be removed from the routing table

Now let's take a look at how to add and remove a routing path from the local routing table using the netsh command.

The "netsh interface add route" command adds a routing path to the local routing table.

The "netsh interface delete route" command removes a routing path to the local routing table.

Arp -s adds the host associated with the given IP address and its corresponding MAC address as a permanent entry.

Arp -d deletes the host associated with the given IP address and its corresponding MAC address. Arp -d * deletes all arp entries in the table.

The "flushdns" option resets the DNS cache, discarding entries.

The "Registerdns" option manually initiates dynamic DNS registration for hosts and IPs on the system.

The "nestsh dnsclient add dnsserver" command will add a new DNS server to the system configuration. If the command is successful, there should be no output from the "netsh dnsclient add dnsserver" command.

We can see the new DNS server is listed on the interface.

The "netsh dnsclient delete dnserver" option removes the supplied IP address as a DNS entry to the specified local area connection.

If the command is successful, there should be no output from the "netsh dnsclient delete..." command.

Now, we see that the DNS server has been deleted. Only the new one that we added remains.

The nslookup command will query the default DNS server to obtain domain name and IP address relational information.

The -p option for netstat allows you to specify the protocol to display, so you could specify tcp, udp, tcpv6 or udpv6.

Section Completed

Networking and Name Resolution: Section 3 Transcript

Name Resolution

Name resolution means successfully mapping a machine name to an IP address. There are two types of names: hostnames and NetBIOS names. Click the two names to learn about the characteristics of each type.

Hostname:
A hostname is an alias that is assigned to an IP node to identify it as a TCP/IP host. The hostname can be up to 255 characters long and can contain alphabetic and numeric characters and hyphens. A hostname may be in the form of an Alias or Domain Name.

NetBIOS name:
A NetBIOS name is a 16-byte address used to represent a single computer or a group of computers. The first 15 characters may be used for the name and the 16th character is reserved for use by the services that a computer offers to the network.

Hostname Resolution

The name resolution process employs standard assets to resolve a string to an IP address. To determine which asset is queried first, the system checks whether the string represents an IP address, and then it checks whether the string is a hostname or a NetBIOS name.

Here is what happens when a system attempts to resolve a hostname.

- Windows checks whether the hostname is the same as the local hostname.
- If the hostname and local hostname are not the same, Windows searches the DNS client resolver cache. During system initialization the DNS Resolver Cache is loaded with the contents of the Hosts file.
- If the hostname cannot be resolved using the DNS resolver cache, Windows sends DNS Name Query Request messages to its configured DNS servers.
- If the hostname is a single-label name (i.e., server1) and cannot be resolved using the configured DNS servers, Windows converts the hostname to a NetBIOS name and checks its local NetBIOS name cache. The hostname must be less than 16 bytes long on a Windows system so that they are compatible with NetBIOS name resolution. For converted hostnames less than 15 characters, padding can be added by using special characters to create the first 15 bytes of the NetBIOS name. Windows then adds the NetBIOS services suffix (0x00) as the last or 16th byte. Every Windows-based computer running the workstation service registers its computer name with a 0x00 as the last byte. Therefore, the NetBIOS form of the hostname will typically resolve to the IPv4 address of the computer with the matching hostname.
- If Windows cannot find the NetBIOS name in the NetBIOS cache, Windows contacts its configured WINS servers.

- If Windows cannot resolve the NetBIOS name by querying its configured WINS servers, Windows broadcasts as many as three NetBIOS Name Query Server Requests messages on the directly attached subnet.
- If there is no reply to the NetBIOS Name Query Request messages, Windows searches the local Lmhosts file.
    1. The name resolution process stops when Windows finds the first IP address for the name. If Windows cannot resolve the hostname using any of these methods, then name resolution fails. If this happens, there are only two ways to communicate with the destination host: specify either its IP address or specify another hostname associated with the unresolved host.

NetBIOS Name Resolution

NetBIOS name resolution is the process of successfully mapping a NetBIOS name to an IPv4 address. Here is how this works:

- When a NetBIOS application such as net.exe needs to resolve a NetBIOS name to an IPv4 address:
    - NetBT checks the NetBIOS name cache for the NetBIOS name-to IPv4 address mapping of the destination host.
    - If NetBT finds a mapping, the NetBIOS name is resolved without generating network activity.
- If the name is not resolved from the entries in the NetBIOS name cache, NetBT attempts to resolve the name through three NetBIOS name queries to each configured NetBIOS Name Service (NBNS), also called WINS.
- If the configured NBNSs do not send a positive name response, NetBT sends up to three broadcast queries on the local network.
- If there is no positive name response and the Use LMHOSTS Lookup check box in the WINS tab is selected, NetBT scans the local Lmhosts file.
- If the NetBIOS name is not resolved from the Lmhosts file, Windows attempts to resolve the name through hostname resolution techniques.
    - NetBT converts the NetBIOS name to a single label, unqualified domain name by taking the first 15 bytes of the NetBIOS name and removing the spaces from the end of the name. For example, for the NetBIOS name FILESRV1[20], the corresponding single-label, unqualified domain name is filesrv1.
- If the converted NetBIOS name does not match the local hostname, the DNS client service checks the DNS client resolver cache.
- If the name is not found in the DNS resolver cache, the DNS Client service attempts to resolve the name by sending queries to a DNS server. The DNS Client service creates fully qualified names from the converted NetBIOS name (single-label, unqualified domain name).
- If none of these methods resolves the NetBIOS name, NetBT indicates an error to the requesting NetBIOS application, which typically displays an error message to the user.

NetBIOS Name

NetBIOS name types describe the functionality of each name entry. Each entry has a suffix and a type which helps define the name and identify its purpose.

For example, the Unique type indicates that the name may have only one IP address assigned to it. On a network device, multiple occurrences of a single name may appear to be registered. The suffix may be the only unique character in the name.

The Group type indicates that a single name may exist with many IP addresses. Windows Internet Name Service (WINS) responds to a name query on a group name with the limited broadcast address (255.255.255.255). Because routers block the transmission of these addresses, the Internet Group was designed to service communications between subnets.

When a NetBIOS host initializes itself, it registers its NetBIOS names using a NetBIOS name registration request message. The NetBIOS host performs name registration by sending a broadcast message on the local subnet or a unicast message to the NetBIOS name server (NBNS).

Tools

Identifying the services on well-known ports and the process for name resolution can reveal a lot of information about the machines on the network. There are many tools we can use for Windows network awareness. We will only detail a few of these tools; click each tool to learn more. See the Resources for this module for more information.

Arp:
Displays and modifies the IP-to-Physical address translation tables used by Address Resolution Protocol (ARP).

Ping:
Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution.

Pathping:
A route-tracing tool that combines features of the ping and traceroute commands with additional information that neither of those tools provides. The pathping command sends packets to each router on the way to a final destination over a period of time, and then computes results based on the packets returned from each hop.

Tracert:
A route-tracing utility used to determine the path that an IP packet has taken to reach a destination.

Netstat:
Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, netstat displays active TCP connections.

Route:
Displays and modifies the entries in the local IP routing table. Used without parameters, route displays help.

Nbtstat:
Displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache. Nbtstat allows a refresh of the NetBIOS name cache and the names registered with Windows Internet Name Service (WINS). Used without parameters, nbtstat displays help.

Netstat Options

Let's focus a little more now on netstat and the different options you can run. When you run netstat, you will automatically see all the active connections. Here are the useful options to see more information:

- -a adds all listening ports
- -n provides numeric information
- -o lists the owning PID
- -b displays the name of the executable associated with the port
- -r shows the routing table
- -e can help identify if there is an irregular amount of traffic
- -s can be used with -e to provide more detail about the traffic
- -p shows connections or statistics for a particular protocol you have specified

Now, in your Windows VM, run some of these netstat options to familiarize yourself with what this tool provides you.

Using Netstat to Map Listening Ports

Hopefully you feel a little more comfortable with using and viewing a netstat table. The netstat tool can also be used to map listening ports to startup if you are uncertain about the identity of the connection. To do that, you could use the following process. Keep in mind, this is only one example and there may be other ways to get the same result.

Run netstat-ano command to identify the Process ID (PID)
Run tasklist command to display a list of applications and services with their PID for all tasks that are running
Run listdlls on a specific PID to identify DLLs loaded into that process

Now, you try it. Again, in your Windows VM, run these netstat options and familiarize yourself with the outputs.

Exercise Introduction

It is time for an Exercise. In order to successfully complete the Exercise, you are expected to use your notes and any available resources presented throughout the course, in addition to conducting your own Internet research.

Networking and Name Resolution: Section 4 Transcript

Summary

You have completed the Networking and Name Resolution module.

During this module we discussed the standard Windows networking services and the process of Windows Name Resolution.

You should now be able to:

- Describe common Windows networking services and ports,
- Demonstrate ability to use Windows networking commands,
- Identify common commands when using the Netstat tool,
- Demonstrate ability to map listening ports to startup location,
- Explain DNS and NetBIOS Name resolution, and
- Explain the difference between host names and NetBIOS names.

To receive credit and advance to the next module, you must achieve a passing score on the Module Exam. Click the Next Section button to begin the Module Exam.