

Task 1: Utilising ARP and Routing Tables

ARP Stands for "Address Resolution Protocol." ARP is a protocol used for mapping an IP address to a computer connected to a local network LAN. Since each computer has a unique physical address called a MAC address, the ARP converts the IP address to the MAC address.

The ARP table 'maps' logical IP (Internet Addresses) to Physical Addresses of Network Interfaces, this is how a packet is sent/received on a Network Interface, or if you like, how packets arrive at your machine over the Internet.

[On the Server 1 VM]:

Click Start – run – cmd and at the command prompt type ARP -A

The information you see displayed comprises of:

- ☐ The Interface (NIC's) in your Machine.
- ☐ The Physical (MAC) Address of this NIC
- ☐ The Internet Address of this NIC.

You may not at present have any (or you may have very few entries). As you connect to, are connected to; other servers, this ARP Table (MAC Table) will be updated; One common way to see this in practice, is by using an ICMP operation such as 'PING'

To verify what networks your host is connected to, you can use the route print command to print out the Routing Table information on your operating system. o Click Start – run – cmd and at the command prompt type route print

Task 2: Remote access to server from Client Machine

Ans: Video Lecture

Task 3: Installing and configuring the Routing and Remote Access Service

[On the Server 1 VM]:

- o Open Server Manager – Add roles and features.
- o Role based or feature based installation – Click Next
- o Select a Server from the Server pool (choose your server1 Server) - click Next
- o At the Select Server Roles screen – check on Remote Access choose Next
- o Do not make any changes in Features and click on Next.

In Role services, select DirectAccess and VPN, Routing services and click on Next.

- o Review installation page and click on install once you are ready.

- o Once the installation is completed, click the link 'Open the Getting Started 'Wizard'
- o At the 'Configure Remote Access' wizard screen - click on Deploy VPN only
- o You should now be brought to the Routing and Remote Access Window:
- o Right click on the icon with your Servername listed – choose Enable and Configure Routing and Remote Access.
- o Choose Next at the Welcome wizard
- o At the Configuration wizard screen, select 'Custom Configuration'
- o Choose LAN Routing – click Next
- Click on Start service.

Task 4: IP Packet Filtering

IP Packet filtering is Microsoft's basic firewall configuration service. It is able to restrict packet flow by utilising a combination of source/destination ports and the protocol that these services use. Packet filtering uses two concepts known as Inbound and Outbound Filters. Inbound Filters are a rule which apply to the Firewall/Router (In our case, Server 1). Outbound filters are concerned with packets that are trying to leave the Router's/servers.

Filter 1: Stopping 'anyone' in Private net from Pinging the Router Firewall Service.

- o Open Server Manager – Tools – Routing and Remote Access.
- o In the left hand console window, expand your Server Name if needed and click to expand IP Routing – Then Click General
- o Right click the PrivateNet1 Connection interface, click Properties.
- o Click Inbound Filter (anything coming into the Router on the PrivateNet1 Connection interface).
- o Choose New
- o Check on Destination Network
- o IP Address: 192.168.100.1
- o Subnet Mask: 255.255.255.255 (This mask value is applied, since we know the EXACT HOST that we want to affect by our rule).
- o Protocol: ICMP
- o Click Ok (leave the last two fields ICMP code and type empty, the filter will include these itself).
- o Ensure that the following option is checked 'Receive all packets, except those

that meet the criteria below'

Observational Tasks

NB: You should use a proper referencing style here when submitting your answers.

Task 3

3 a) How do Router's reference which networks they are able to connect to?

A router helps to connect multiple devices to the Internet, and connect the devices to each other. Also, you can use routers to create local networks of devices. These local networks are useful if you want to share files among devices or allow employees to share software tools.

Task 5:

a) Failover Clustering for high availability systems/services. A failover cluster is a set of physical or virtual computer systems that work together to facilitate a High Availability (HA) or Continuous Availability (CA) environment for the various applications and services that run within enterprise networks.

Windows Server Failover Clustering (WSFC) is a feature of the Windows Server platform for improving the high availability (HA) of applications and services. ... In order for a failover cluster to work, each server's hardware specifications must be the same and the servers must share storage.

What is Hyper-V failover cluster? Failover cluster is a set of several similar Hyper-V servers (called nodes), which can be specifically configured to work together, so that one node can take the load (VMs, services, processes) if another one goes down or if there is a disaster.

5 a) Give a detailed explanation of the concepts that need careful consideration when considering the usage of such a system. Also show one possible role within the Window Server OS environment that could provision these requirements. **YOU DO NOT HAVE TO BUILD, DEPLOY OR TEST A FAILOVER CLUSTER.**

Answer hints:

To mitigate system downtime and ensure high availability for Windows, IT best practice recommends that you cluster servers (or nodes) so that if one node fails, one or more other nodes automatically take over-processing. This is also referred to as Windows clustering.

Task 6:

Observational Tasks

6 a) Assume that you are the Head - Network Administrator of an Enterprise Network which operates in multiple locations nationwide. Draft a network policy, Critical business applications high availability practices and security practices for your network. State all

assumptions made. (Hint: In your draft, address (not limited to) the architecture/ topology/ design/ layout of the network, network access, security team, enforcement of security policies, analysis of security risks, scope of security changes (if needed), monitoring the security operations, mitigations in the event of violations, etc)