Welcome! To the Starship SNS GMISprise
Welcome aboard the Starship
“SNS GMISprise!”
We will be guiding you through your training to become the next great AZ-700 red shirt engineer!
To boldly go....to the cloud..

For the next few hours we will have you aboard as we train you for the Microsoft AZ-700 Azure Associate Network Engineer exam. So prepare yourself as it is time to be beamed aboard the SNS GMISprise!
To boldly go....to the cloud..

Well, I guess you will just have to stay in your seats instead.....but in any case we will get you through the semantics of this course and you are welcome to ask any question at anytime!
First things first....

• Class time
• Bathrooms
• Food / Drink
• Please contribute! We encourage discussion!
• Questions always welcome! Ask anytime!! You may interrupt! We’re here to help!
First things first....

• Who: StarNet Solutions, member & sponsor of GMIS since 2015
• Where: Class M planet in a city called Farmingdale, NJ but we travel the galaxy, well at least worldwide!
• What: Any IT except writing applications or building webpages.
• Yes, CUSTOMERS COME FIRST!
• We are Booth #35!
Exam Details:

- You have about 2 hours to complete the exam.
- It is between 50-60 questions.

- Understanding to design and implement core networking infrastructure (20–25%)
- Understanding to design, implement, and manage connectivity services (20–25%)
- Understanding to design and implement application delivery services (20–25%)
- Understanding to design and implement private access to Azure services (5–10%)
- Understanding to secure network connectivity to Azure resources (15–20%)

- ** There are constant updates so these may change over time! **
Exam Details:

How......

- ...many people here are using O365/M365?
- ...many people have virtualized pcs or servers in Azure?
- ...many people have moved all of their entire on-premise systems to the cloud?
Quick Azure AD Review:

- Azure AD is Microsoft’s cloud-based identity and access management service to help users sign in and access resources.
- Internal Apps: Applications on-prem or access to workstations on-prem from the cloud.
- Azure AD allows SSO (Single Sign On) making your life easier.
Quick Azure AD Review (cont.):

- Active Directory was introduced with Windows 2000.
- On-prem AD provides authentication and authorization for on-premise users only.
- Azure goes to the next level by providing IDaaS (Identity as a Service) for everything from the cloud to on-prem.
- Azure AD can provide authentication for on-prem and cloud.
Quick Azure AD Review (cont.):

- Azure AD Connect provides on-prem to Azure AD synchronization: Installed software on-prem.
Networking in Azure:

• How many people are familiar with routing and subnetting?
• Creating networks in Azure will be much easier if you are already familiar with these topics.
• It’s only different from what you do on-prem in that some of the terms and ways in which you configure them exist.
• But... networking is networking and TCP/IP has standards and rules which everyone must abide by or things do not work!
Networking in Azure:

- Virtual networks (VNET):
  - A virtual (initially) isolated network in Azure that can be further subnetted to allow networks to communicate.
  - VNETs can be connected to other VNETs in Azure, outside resources or kept private and secluded to only their own arena.
  - All typical functions of a network are available just like a network in your office. DHCP, DNS, routing, virtual machines, etc. are all functional in a VNET.
Networking in Azure:

- Virtual networks (VNET) Example:
  - BASICS OF VNETS:
    - VNETs can be further divided into subnets.
    - Subnets can talk to each other with no additional configuration.
    - These subnets are isolated to each other within this VNET unless additional configuration is provided to permit them to go outside of their VNET.
    - VNETs are secure from outside resources.
Networking in Azure:

• Virtual networks (VNET) Example:

BASICS OF VNETS:

• VNICs are the virtual network interface cards (adapters) on a virtual machine in Azure. Each virtual machine will have one.

• NSG stands for: Network Security Group.
  • This is an IP Filter and *NOT* a firewall. It is a basic IP filtering virtual device.

• NSGs can be placed on the entire subnet or on the VNICs themselves.

• The purpose of the NSG is to allow or deny network (IP) traffic between devices or subnets.
Networking in Azure:

- Virtual networks (VNET) Peering Example:

BASICS OF VNETs: Each of these VNETs are isolated from each other but the subnets within each VNET can communicate natively.
Networking in Azure:

- Virtual networks (VNET) “special” subnets:
  - Some devices you want to use in your Azure networking such as an Azure VPN Gateway or Azure Firewall. These will require their own subnets. They cannot be part of the same subnet(s) that you are using for other things, but they will be part of the same VNET.
  - There are devices like Azure Application Gateways that can use the same subnet as your existing devices.
  - When you create such devices, the wizard will provide feedback so you know.
Networking in Azure:

• Virtual networks (VNET) Subnet Delegation:

• “Subnet delegation enables you to designate a specific subnet for an Azure PaaS service of your choice that needs to be injected into your virtual network. Subnet delegation provides full control to the customer on managing the integration of Azure services into their virtual networks.”

• - Learn.Microsoft.com
Networking in Azure:

• Virtual networks (VNET) Considerations:

  • Plan your address space if you are connecting your on-premise network to Azure.
  • Overlapping networks will be a headache!
  • VNETs can be used to secure systems such as SQL servers, email servers, file servers, etc. or whatever you choose.
  • Peering can be in the same region (Virtual Network Peering) or across Azure regions (Global Virtual Network Peering)
  • Peering provides low latency connections between different VNETs.
Networking in Azure:

• Let’s Do Some Show and Tell in Azure!

• Off to portal.azure.com!
Virtual Network Creation
VNET Peering
VNET Subnet Delegation
Networking in Az

• Public IP Address Spaces and Public Prefixes
  - You can create reserved public spaces in advance or at any time to reserve public Azure IP addresses.
  - These will be useful if you are planning to connect your office to Azure via vpn, for setting up services and documenting them prior to creation, etc.
  - These addresses are available in blocks of 2, 4, 8, or 16.
  - You can also use your own addresses (CUSTOM) instead of the Microsoft provided ones...say what??!!!
Networking in Azure:

- Custom Public IP Address Spaces

  You can use your existing Public IP addresses in Azure. Perhaps you have had them for many years and changing the IP addresses is an incredibly arduous task and this offers an alternative.

  The process is you permit Azure to advertise your IP address space as your own.

  Requires you to send in an ROA, Route Origin Authorization form.

  Once you have this completed, you will receive an SSL cert, and then you can create your Public IP prefix.
Networking in Azure:

- Custom Public IP Address Spaces (cont.)
- After that you can deploy, but the entire process may take up to TWO WEEKS to complete.
- The addresses can only exist within ONE region.
- You cannot advertise these routes over ExpressRoute
Networking in Azure:

• Custom Public IP Address Spaces (cont.)

• You cannot move these addresses to another subscription or Resource Group once they are assigned.
Public Prefix Creation
Public IP Address Assignment
Networking in Azure:

• Connecting Azure to On-Prem

• Essentially we have two ways to do this:
  • VPN: using an Azure VPN gateway (or a 3rd party Azure based vpn gateway.)
  • ExpressRoute (a direct connection)
Networking in Azure:

• Connecting Azure to On-Prem: VPN

• This requires the use of a vpn between your on-prem firewall or vpn concentrator and an Azure VPNGateway or 3rd party gateway (vpn, firewall, router) in the Azure cloud.

• Less expensive than ExpressRoute
Networking in Azure:

- Connecting Azure to On-Prem: VPN
Networking in Azure:

- Connecting Azure to On-Prem: ExpressRoute

- ExpressRouter requires equipment to be installed in your office that bypasses the Internet and puts a direct connection between your office and Microsoft Azure. It is much more expensive and usually done by very large enterprise organizations if needed.
Networking in Azure:

• Connecting Azure to On-Prem: VPN

AZURE CONNECTION EXAMPLE

ExpressRoute

INTERNET

FIREWALL

Your Building
BREAK TIME....
GAME TIME!!!

What is this creature called?

GORN
GAME TIME!!!

Complete this statement:

“Set _______ to stun!”

PHASERS
GAME TIME!!!

What episode was this probe from:

THE CHANGELING – EPISODE #37, 1967
Networking in Azure:

• How about some DNS?

• Both Private and Public DNS servers are available with Azure.
• Creating virtual machines inside of Azure will assign a private DNS name unless you specify your own custom domain.
• Opening a device with a public IP address in Azure will assign a public DNS name that is owned by Microsoft Azure services.
• However, you can change this to use your own private or publicly hosted DNS servers to use specific domains you own.
• Each VNET can have its own custom DNS servers and zones.
Networking in Azure:

• How about some DNS? (cont.)

• DNS in Azure is simply linked to the zone or pointed to your outside hosted DNS servers.
• If you want to use your public FQDN, you will have to follow a similar process to verify you own it – similar to what you did if you moved to O365.
• Private DNS for VNETs can allow things like virtual machines in the cloud to self register into DNS.
Networking in Azure:

- Private DNS Resolver
- What happens if you have private on-premise DNS and you want to connect it to Azure so that you can forward requests to/from Azure?
- In this case you would use the Azure Private DNS Resolver. This allows zone records to be sent back and forth between Azure and your on-premise DNS servers.
Networking in Azure:

- Private DNS Resolver

- Prerequisite: Must have connection to Azure via VPN or Expressroute

- Prerequisite: You must have at least two subnets in Azure. The allows for the creation of an inbound endpoint on one subnet and an outbound endpoint on the other.
Networking in Azure:

• More Show and Tell....!

• Off to portal.azure.com!
**DNS Private Resolver Creation**

![Microsoft Azure Portal](image.png)

**Azure services**

- Create a resource
- DNS private resolver
- Private DNS zones
- DNS zones
- Virtual machines
- Public IP Prefixes
- Resource groups
- Virtual networks

**Resources**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Last Viewed</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMISDemosResGp01</td>
<td>Resource group</td>
<td>10 minutes ago</td>
</tr>
<tr>
<td>Azure subscription 1</td>
<td>Subscription</td>
<td>39 minutes ago</td>
</tr>
<tr>
<td>GMISDemosPublicIP01</td>
<td>Public IP Prefix</td>
<td>8 hours ago</td>
</tr>
<tr>
<td>VNetC</td>
<td>Virtual network</td>
<td>12 hours ago</td>
</tr>
<tr>
<td>VNetA</td>
<td>Virtual network</td>
<td>12 hours ago</td>
</tr>
<tr>
<td>VNetG</td>
<td>Virtual network</td>
<td>12 hours ago</td>
</tr>
</tbody>
</table>

**Navigate**

- Subscriptions
- Resource groups
- All resources
- Dashboard
Networking in Azure:

• Creating VPNs To & from Azure

• You will need an Azure VNETgateway.
• Azure VNETgateways will always have their own dedicated subnet in your VNET.
• There are two types:
  • Route based
  • Policy Based
Networking in Azure:

- Do Tell Us More!....!
- Off to portal.azure.com!
VNETgateway Creation
Networking in Azure:

- Creating VPNs To & from Azure
- **Powershell**: `New-AzIpsecPolicy`
- Required for Policy Based vpns in Azure.

Networking in Azure:

- Azure Firewall (3 types/skus):
  - Basic – least expensive, least amount of features
  - Standard – more expensive, more features
  - Premium – most expensive, most amount of features

Networking in Azure:

- Azure Firewall
- Basic:
  - intended for small and medium size (SMB) customers to secure their Azure cloud environments. It provides the essential protection SMB customers need at an affordable price point.

Networking in Azure:

- Azure Firewall
  - Standard:
    - Azure Firewall Standard provides L3-L7 filtering and threat intelligence feeds directly from Microsoft Cyber Security. Threat intelligence-based filtering can alert and deny traffic from/to known malicious IP addresses and domains that are updated in real time to protect against new and emerging attacks.

Networking in Azure:

• Azure Firewall
• Premium:
  • Azure Firewall Premium provides advanced capabilities include signature-based IDPS to allow rapid detection of attacks by looking for specific patterns. These patterns can include byte sequences in network traffic, or known malicious instruction sequences used by malware. There are more than 58,000 signatures in over 50 categories that are updated in real time to protect against new and emerging exploits. The exploit categories include malware, phishing, coin mining, and Trojan attacks.

• https://learn.microsoft.com/en-us/azure/firewall/overview
Networking in Azure:

• Azure Firewall
• Creating Azure Firewalls requires the creation of a subnet in the VNET called “AzureFirewallSubnet”. If you try and create an Azure firewall before this subnet is created, you will NOT be able to create your firewall!
• Hence, create the subnet “AzureFirewallSubnet” in your VNET BEFORE you try and create the firewall.
Networking in Azure:

• Azure Firewall
• Once the firewall is created, you will need to add routes AND associate them to the subnets that want to pass through this firewall.
• They will require you to create rules and policies based on your network needs.
• There are 3 default rule collection groups. They cannot be deleted. However, you can create your own custom rule collection groups to work around them.
Networking in Azure:

• Azure Firewall
• We have 2 types of traffic flow: inbound and outbound
  • Inbound: traffic entering the firewall.
  • Outbound: traffic leaving the firewall.
Networking in Azure:

- **Azure Firewall**
- We have 3 types of firewall rules: DNAT, Network, and Application.
- **DNAT**: translating traffic to/from public to private or vice versa such as inbound traffic to a web or email server.
- **Network**: allowing or denying traffic based on IP addresses and/or ports. (Layer 3/4)
- **Application**: allowing or denying based on applications like URLs, FQDNs, etc. (Layer 7).
Networking in Azure:

• HOW...
  • ...many of you use a layer 7 firewall?
  • ...many of you know the difference?
Networking in Azure:

- Azure Firewall
  - All rules are created by a Firewall Policy.
  - Policies contain rules of DNAT, Networking and Application or any combination of them based on your requirements.
  - Rules are done in priority from 100 to 65000 with 100 being the highest priority.

AZfirewall Creation
Cloud... the Final Frontier...

THANK YOU FOR COMING!

BOOTH 35

PLEASE COME GET YOUR CERT!