AT&T NetBond for Cloud for Microsoft Azure

Service Activation Overview

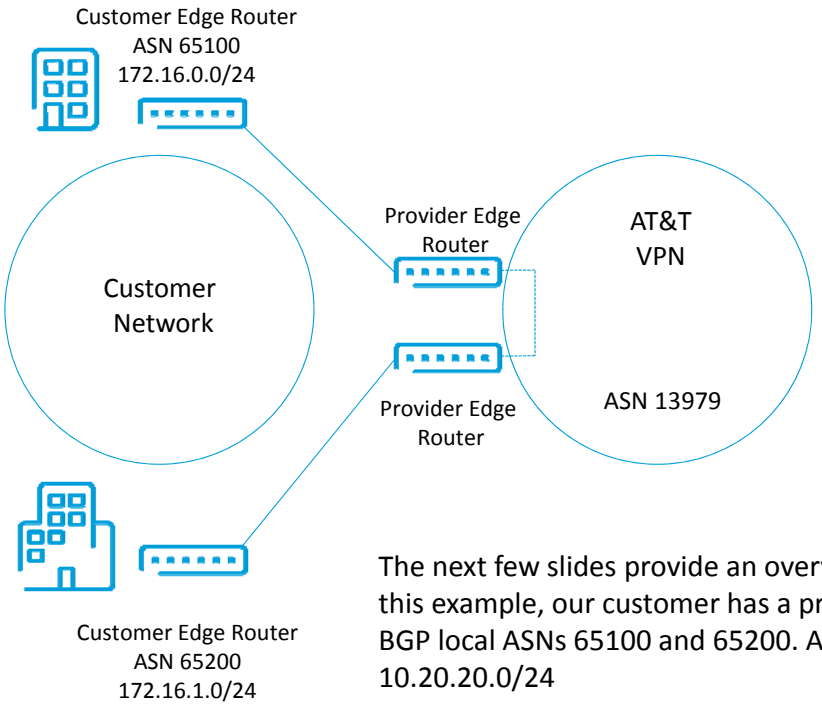
AT&T NetBond® for Cloud allows AT&T customers to extend their MPLS virtual private network (VPN) to cloud services such as Microsoft® Azure®. With NetBond for Cloud enabled, an Microsoft® Azure® Virtual Network or Microsoft Azure public service such as Microsoft® Azure® Blob storage will appear as another site on the VPN. Customers can then reach their virtual machines or blob storage with better scalability, improved security, and greater availability.

Using the AT&T Cloud Solutions portal, the NetBond for Cloud service can be quickly provisioned. The next few slides provide an overview to plan and enable the service.

Prior to enablement, the customer should have or procure service with Microsoft. They should also work with the AT&T account team to sign up for NetBond for Cloud services. Upon contract signing, the customer will receive a welcome email for credentials to www.synaptic.att.com.

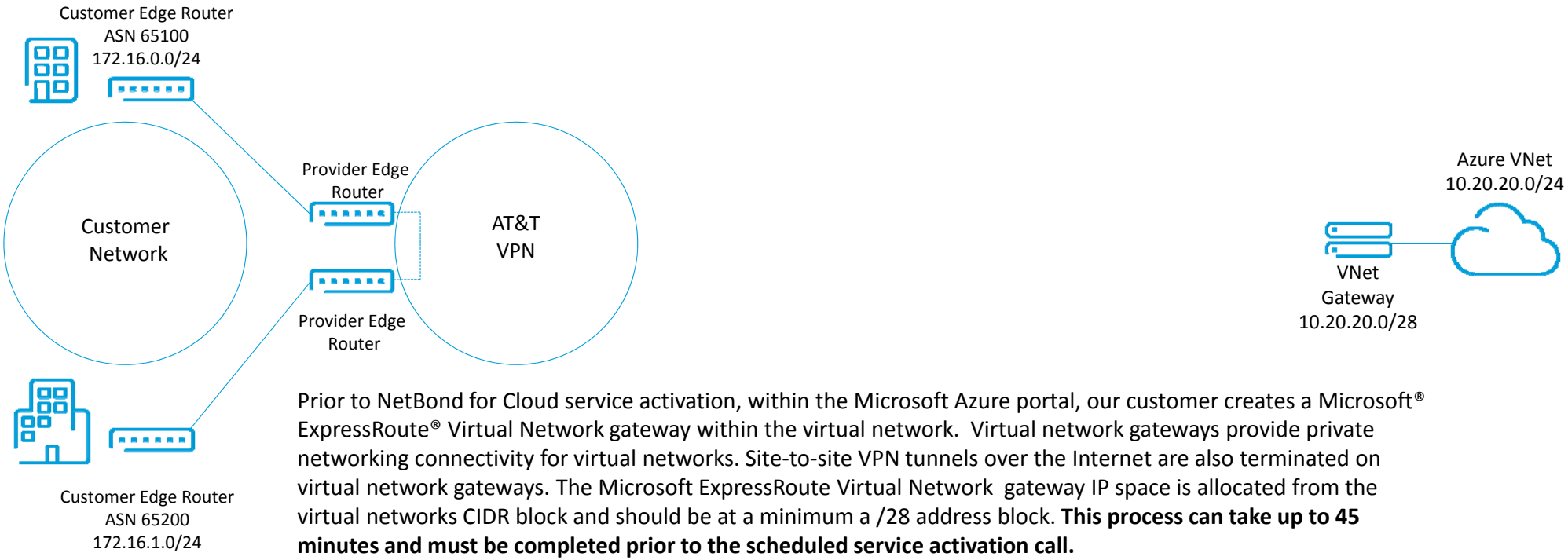
Service Activation Overview for Microsoft Azure Virtual Network

Example Scenario – Customer with existing AT&T VPN and Microsoft Azure Virtual Network



The next few slides provide an overview of a typical service activation with a Microsoft Azure Virtual Network. In this example, our customer has a private network with AT&T VPN service, and two representative U.S. sites using BGP local ASNs 65100 and 65200. An existing Microsoft Azure Virtual Network is ready with an IP address range of 10.20.20.0/24

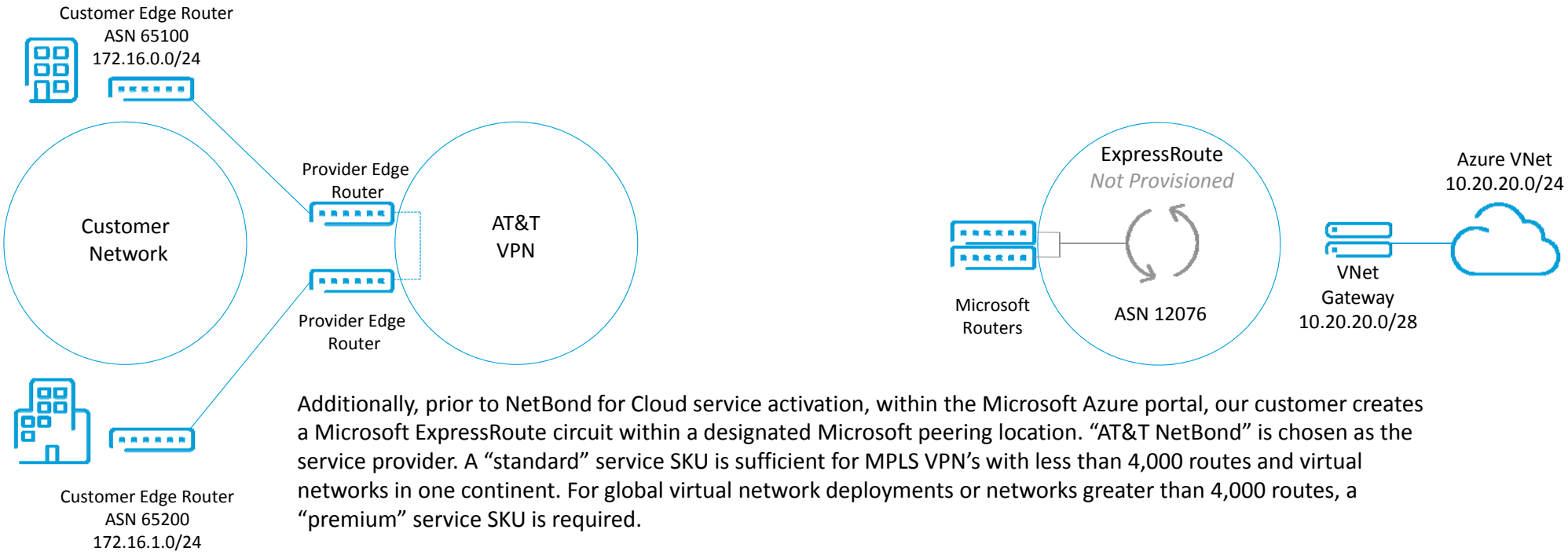
Prerequisite – Create Microsoft ExpressRoute Virtual Network Gateway



Prior to NetBond for Cloud service activation, within the Microsoft Azure portal, our customer creates a Microsoft® ExpressRoute® Virtual Network gateway within the virtual network. Virtual network gateways provide private networking connectivity for virtual networks. Site-to-site VPN tunnels over the Internet are also terminated on virtual network gateways. The Microsoft ExpressRoute Virtual Network gateway IP space is allocated from the virtual networks CIDR block and should be at a minimum a /28 address block. **This process can take up to 45 minutes and must be completed prior to the scheduled service activation call.**

Note: Customers who want to maintain a site-to-site Ipsec tunnel in conjunction with NetBond for Cloud/Microsoft ExpressRoute connectivity should consult with their Microsoft support representative prior to performing this step.

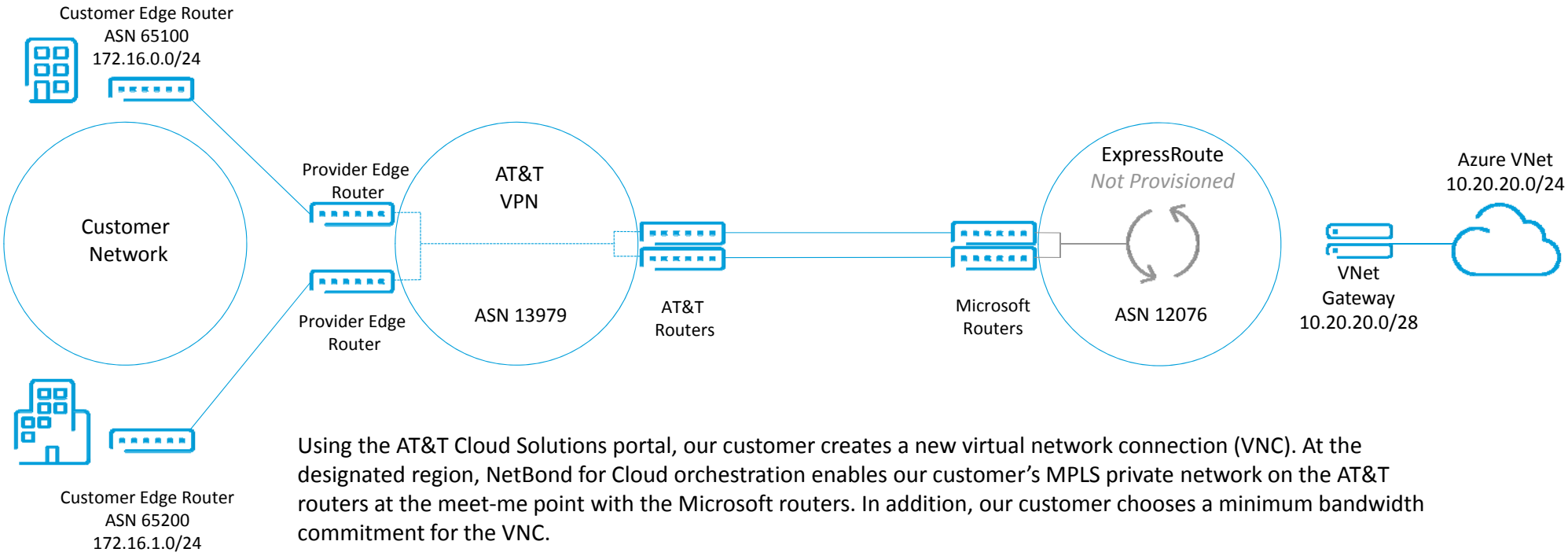
Prerequisite #2 – Create Microsoft ExpressRoute Circuit



Additionally, prior to NetBond for Cloud service activation, within the Microsoft Azure portal, our customer creates a Microsoft ExpressRoute circuit within a designated Microsoft peering location. “AT&T NetBond” is chosen as the service provider. A “standard” service SKU is sufficient for MPLS VPN’s with less than 4,000 routes and virtual networks in one continent. For global virtual network deployments or networks greater than 4,000 routes, a “premium” service SKU is required.

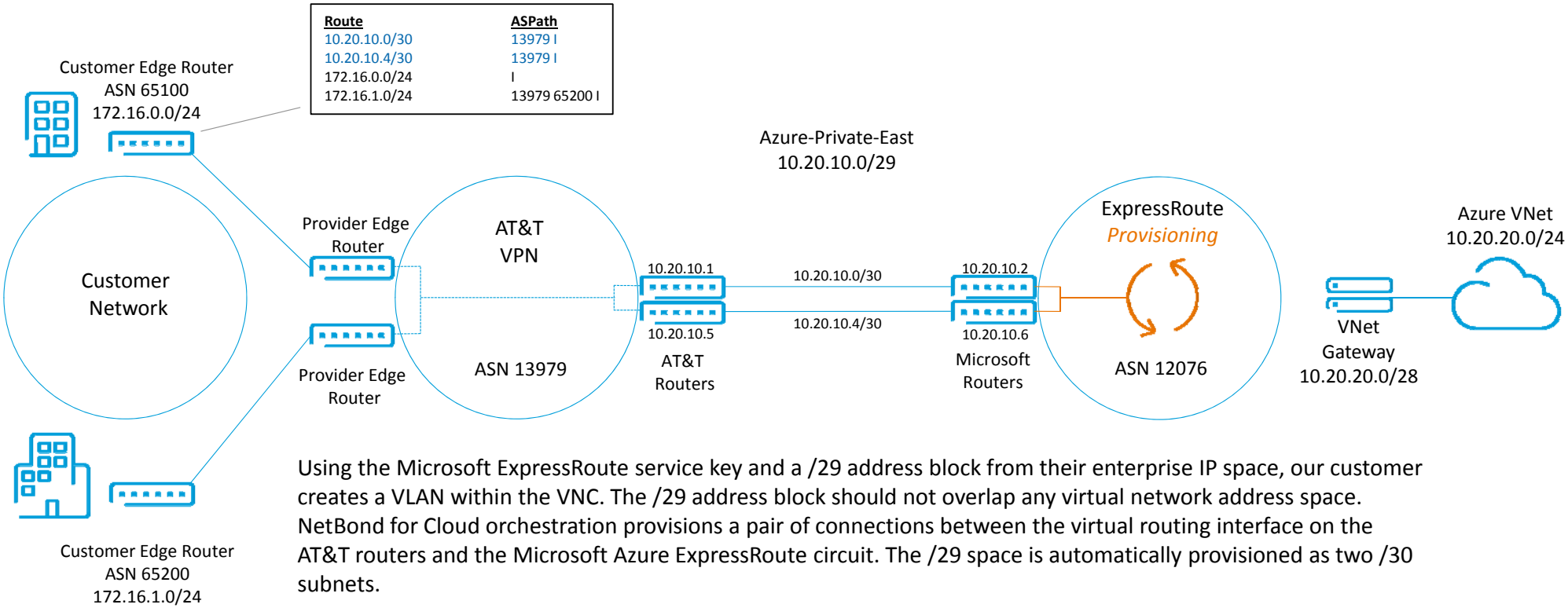
Instructions for creating a Microsoft ExpressRoute circuit can be found at the following link. **Only follow Steps 1-4**.
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-circuit-portal-resource-manager
Once the Microsoft ExpressRoute is created, note the associated service key in the Microsoft Azure portal.

Step 1 – Create Virtual Network Connection (VNC)



Using the AT&T Cloud Solutions portal, our customer creates a new virtual network connection (VNC). At the designated region, NetBond for Cloud orchestration enables our customer's MPLS private network on the AT&T routers at the meet-me point with the Microsoft routers. In addition, our customer chooses a minimum bandwidth commitment for the VNC.

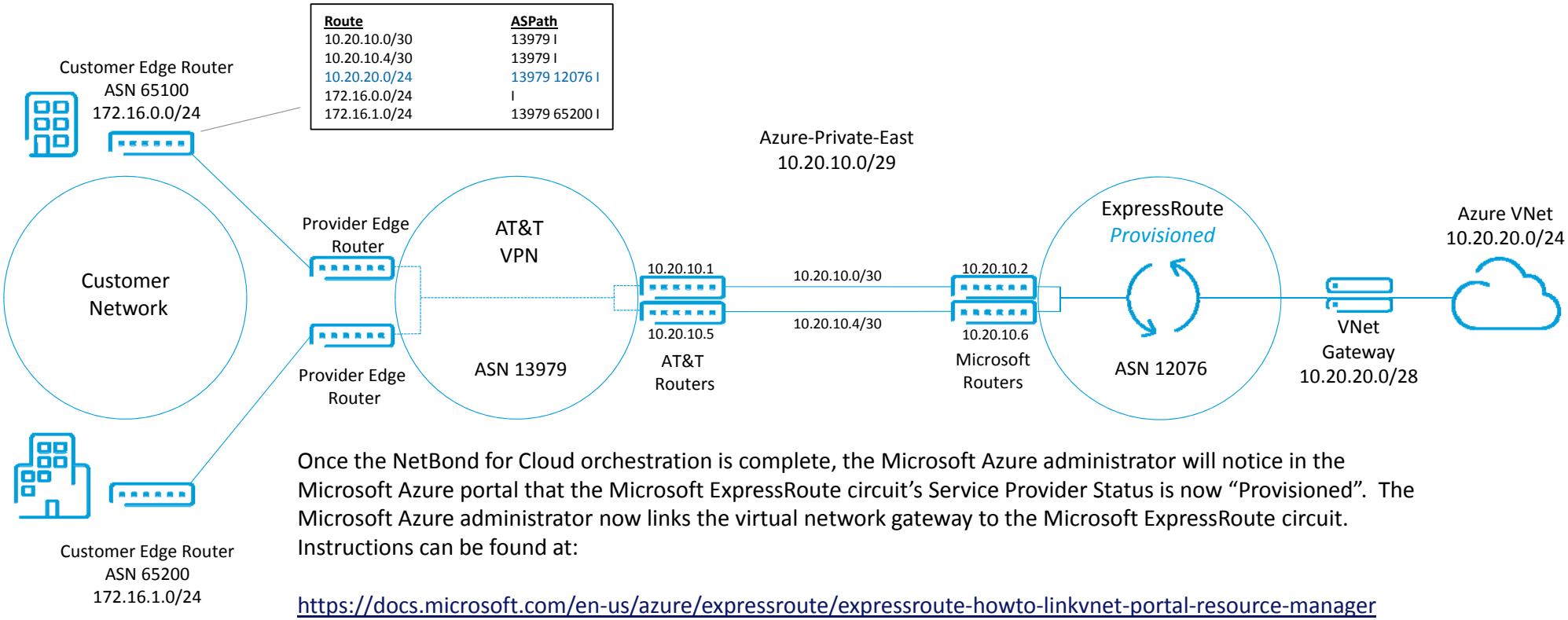
Step 2 – Create VLAN



Using the Microsoft ExpressRoute service key and a /29 address block from their enterprise IP space, our customer creates a VLAN within the VNC. The /29 address block should not overlap any virtual network address space. NetBond for Cloud orchestration provisions a pair of connections between the virtual routing interface on the AT&T routers and the Microsoft Azure ExpressRoute circuit. The /29 space is automatically provisioned as two /30 subnets.

The customer edge routers will now see the /30 subnets in their routing tables. **Note:** Microsoft Azure Virtual Network, (10.20.20.0/24 in the example), will not yet appear since the virtual network is not connected to the Microsoft ExpressRoute circuit.

Step 3 – Connect Microsoft Azure Virtual Network to Microsoft ExpressRoute Circuit



Once the NetBond for Cloud orchestration is complete, the Microsoft Azure administrator will notice in the Microsoft Azure portal that the Microsoft ExpressRoute circuit's Service Provider Status is now "Provisioned". The Microsoft Azure administrator now links the virtual network gateway to the Microsoft ExpressRoute circuit. Instructions can be found at:

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-linkvnet-portal-resource-manager

After a few minutes, Microsoft Azure will finish provisioning the connections to the Microsoft ExpressRoute, and the CIDR block associated with the virtual network will automatically be advertised to all sites on the MPLS VPN.

WARNING! Peering Status and Microsoft ExpressRoute Routing Configuration

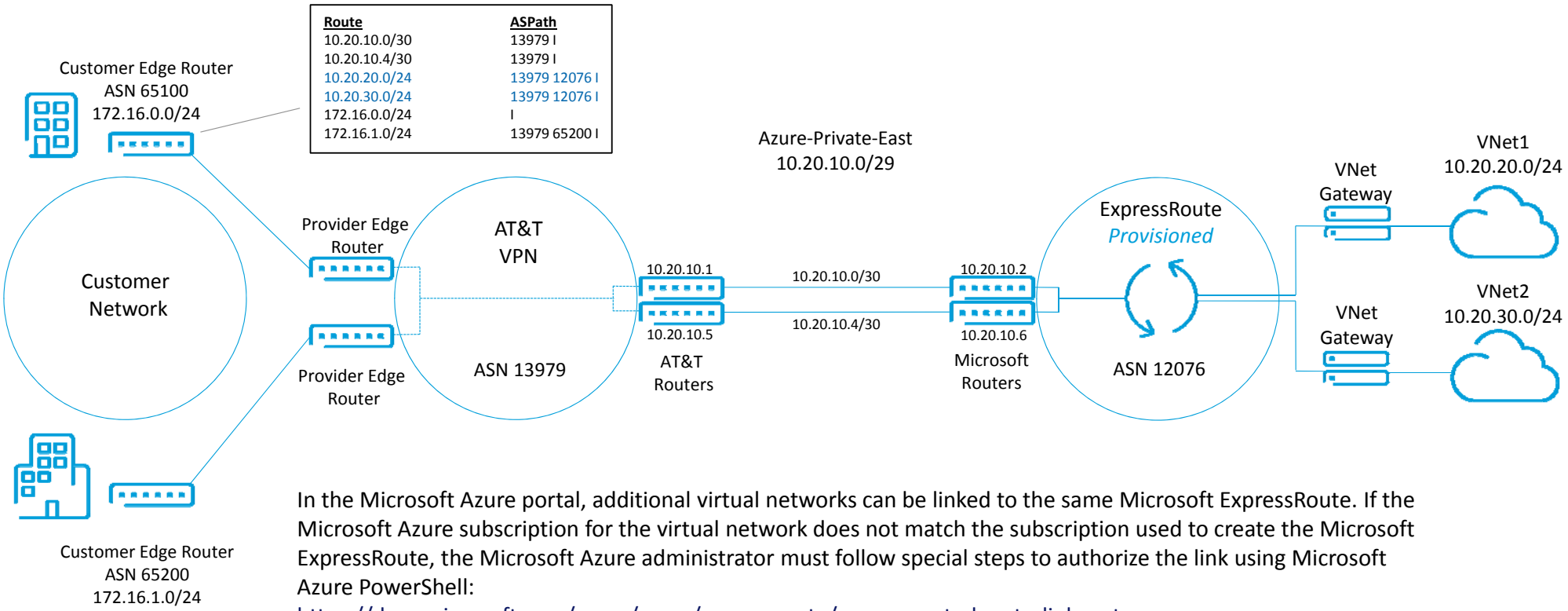
Note that Microsoft does not show BGP configuration information for Layer 3 providers such as AT&T. Per Microsoft's web site:

"We currently do not advertise peerings configured by service providers through the service management portal. We are working on enabling this capability soon."

Additionally, AT&T configures and maintains the Microsoft ExpressRoute routing configuration. Do not configure any of these settings in the Microsoft Azure portal.

Occasionally a Microsoft support representative may incorrectly instruct you to configure the Microsoft ExpressRoute circuit's routing configuration. Under no circumstances should this be done. Instead, remind them that AT&T is a service provider providing managed Level 3 services with Microsoft ExpressRoute.

Additional Virtual Networks



In the Microsoft Azure portal, additional virtual networks can be linked to the same Microsoft ExpressRoute. If the Microsoft Azure subscription for the virtual network does not match the subscription used to create the Microsoft ExpressRoute, the Microsoft Azure administrator must follow special steps to authorize the link using Microsoft Azure PowerShell:
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-linkvnet-arm

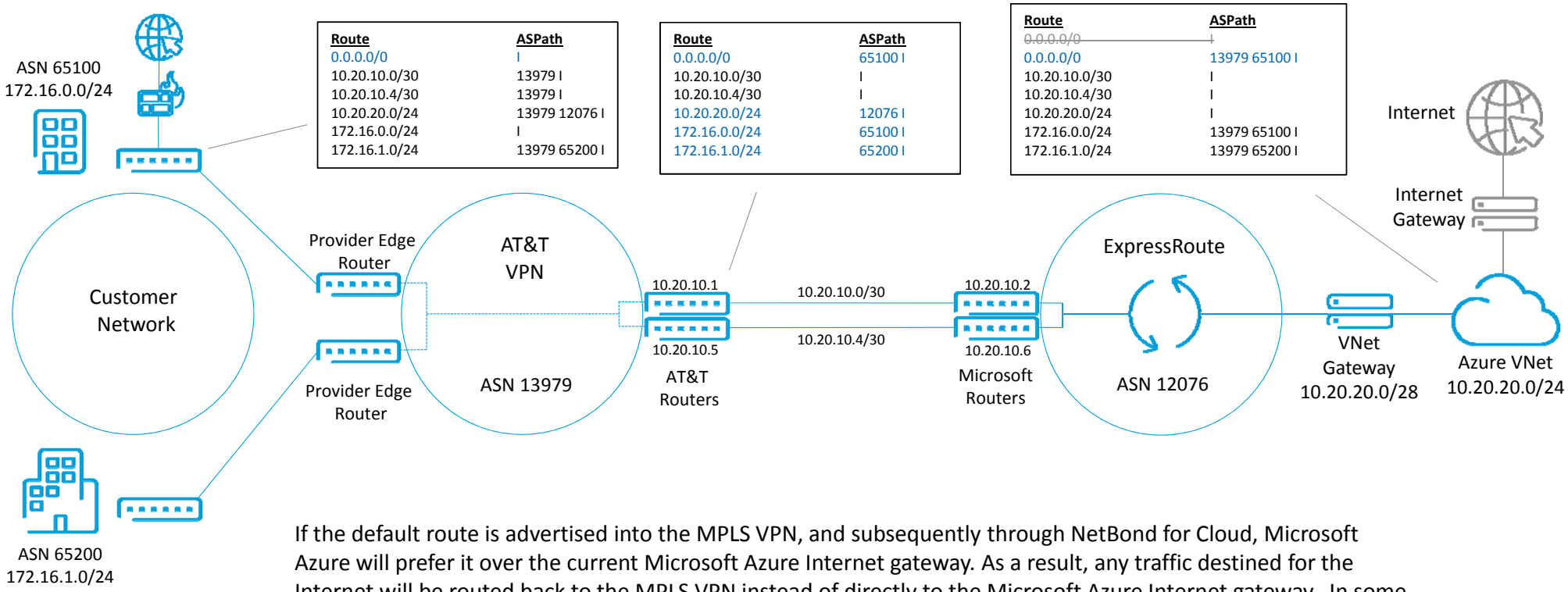
The additional virtual network address space will automatically be propagated to all MPLS VPN sites upon completing the link to the Microsoft ExpressRoute in the Microsoft Azure portal.

Summary Steps

1. Obtain an Microsoft Azure subscription.
2. Work with the AT&T account team to sign up for NetBond for Cloud services. A welcome letter will provide credentials to AT&T Cloud Solutions portal, (www.synaptic.att.com).
3. Within Microsoft Azure, at least one virtual network with an attached virtual network gateway is required.
4. Using the Microsoft Azure portal, create Microsoft ExpressRoute circuit and note the service key.
5. Using the AT&T Cloud Solutions portal, create NetBond for Cloud VNC. (Required: Name of AT&T VPN, region, free-form name for VNC, and minimum bandwidth commitment)
6. Additionally, within the AT&T Cloud Solutions portal, create NetBond for Cloud VLAN. (Required: /29 address space, free-form name, and Microsoft ExpressRoute service key)
7. Link virtual network to Microsoft ExpressRoute through the Microsoft Azure portal.

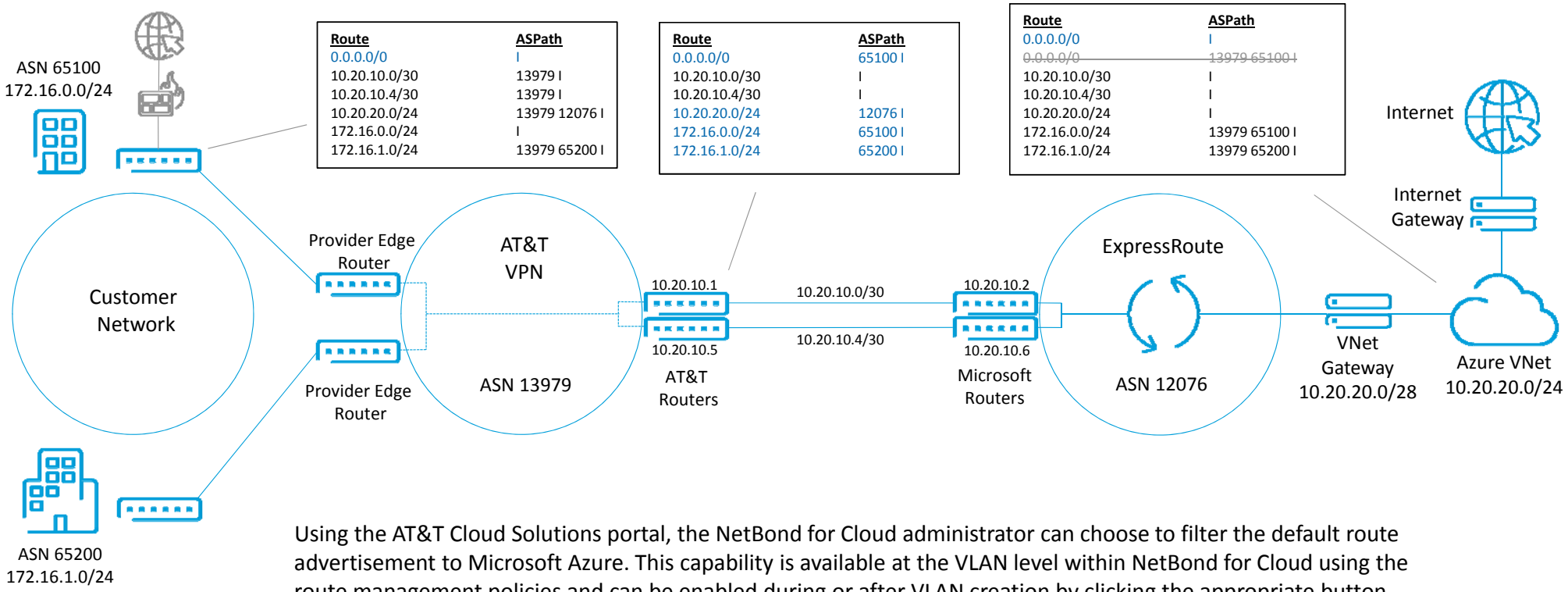
Technical Considerations

Default Route



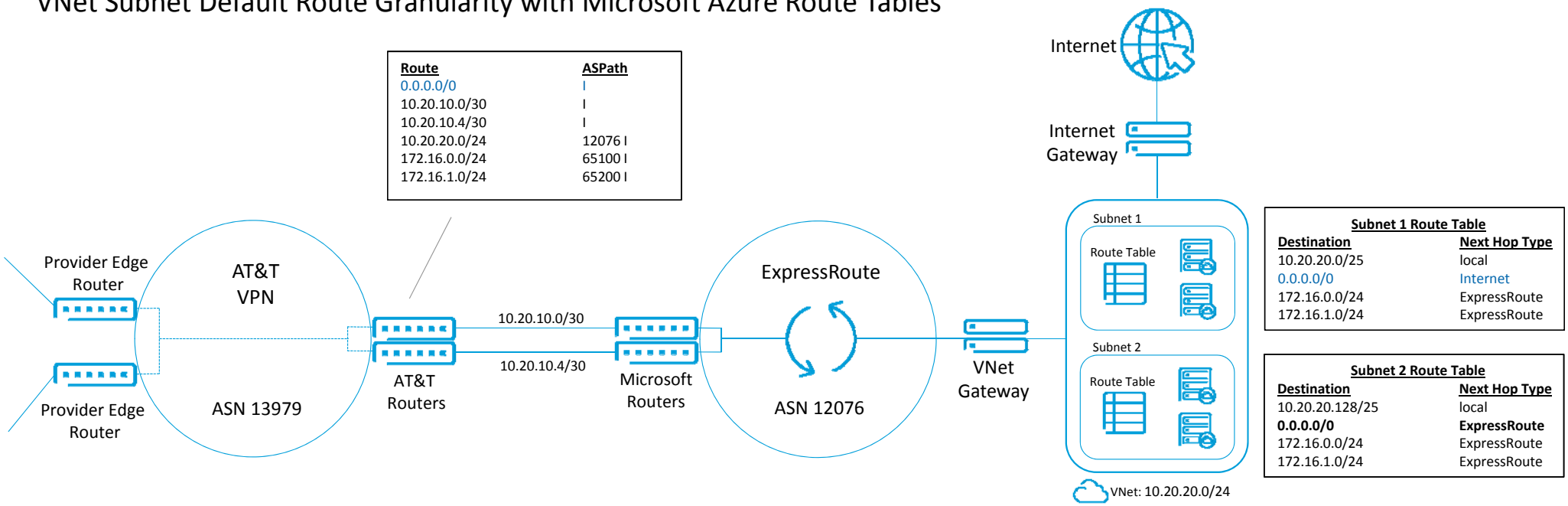
If the default route is advertised into the MPLS VPN, and subsequently through NetBond for Cloud, Microsoft Azure will prefer it over the current Microsoft Azure Internet gateway. As a result, any traffic destined for the Internet will be routed back to the MPLS VPN instead of directly to the Microsoft Azure Internet gateway. In some architectures, this may be the path that you want for Internet traffic. In other architectures where direct Internet access through Microsoft Azure is desired, filtering the default route in the AT&T Cloud Solutions portal is required.

Filter Default Route with AT&T Route Management



Using the AT&T Cloud Solutions portal, the NetBond for Cloud administrator can choose to filter the default route advertisement to Microsoft Azure. This capability is available at the VLAN level within NetBond for Cloud using the route management policies and can be enabled during or after VLAN creation by clicking the appropriate button.

VNet Subnet Default Route Granularity with Microsoft Azure Route Tables



Alternatively, if our customer's Microsoft Azure administrator wants to fine tune which subnets within VNets use the Microsoft Azure Internet gateway, they can use Microsoft Azure user-defined routes to modify the route table of a particular subnet. Any user-defined route within the VNet route table will override any routes learned via Microsoft ExpressRoute. You can find more information about Microsoft Azure user defined routes at: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

In the example above, the administrator chose to have Subnet 1 use the Microsoft Azure Internet gateway by creating a user-defined route for the default route with Next Hop Type of "Internet". **Note:** Microsoft ExpressRoute cannot be designated as a "Next Hop Type". However, routes learned from Microsoft ExpressRoute can be overridden with user-defined routes configured with a target of "Internet", "Virtual Appliance", or "None".

Additional Route Management Capabilities

Through the AT&T Cloud Services portal, NetBond provides additional route policy management features. Use cases include overcoming the Microsoft route limit, (4,000 routes for standard ExpressRoute), backup VNCs for redundancy, or limiting specific routes for security purposes.

Routes advertised by AT&T to Microsoft

- Block the default route
- Limit routes advertised based on a community value applied at the customer edge routers
- Advertise only manually-specified routes
- Prepend route advertisements with extra AS hops

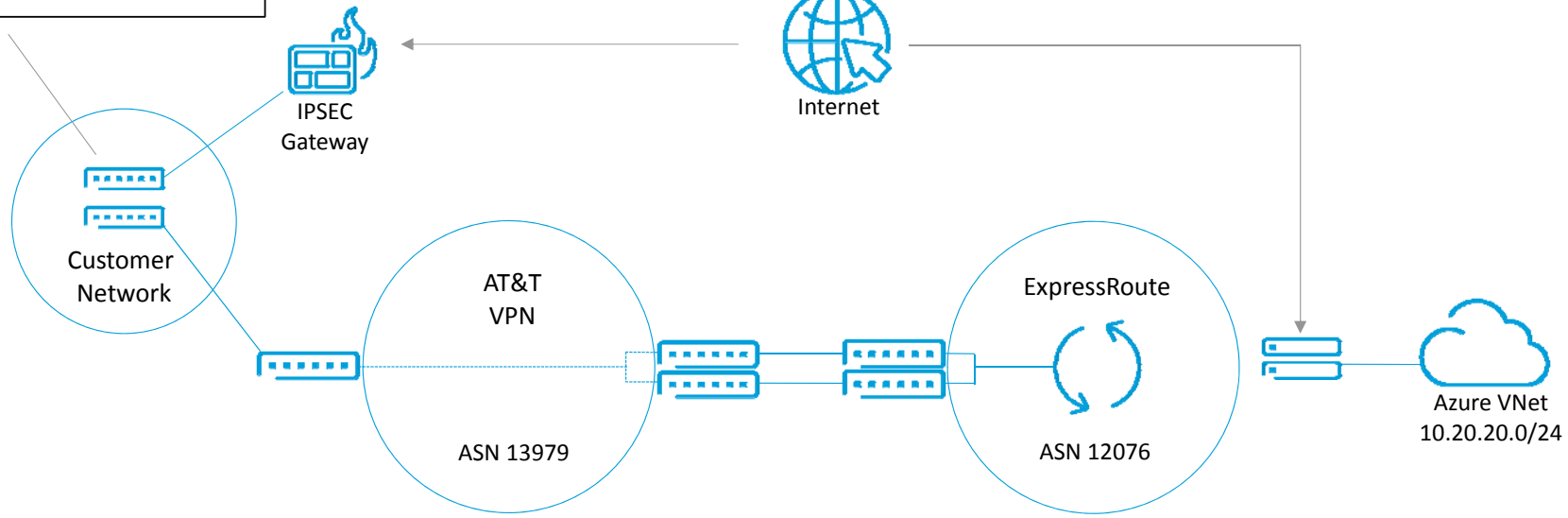
Routes advertised by Microsoft to AT&T

- Block manually specified routes
- Block or allow based on community values applied by Microsoft
- Apply manually-specified community values prior to advertisement to the MPLS VPN
- Prepend route advertisements with extra AS hops
- Advertise only manually-specified routes to the MPLS VPN

AT&T

Migrating from Site to Site VPN Tunnels to NetBond for Cloud

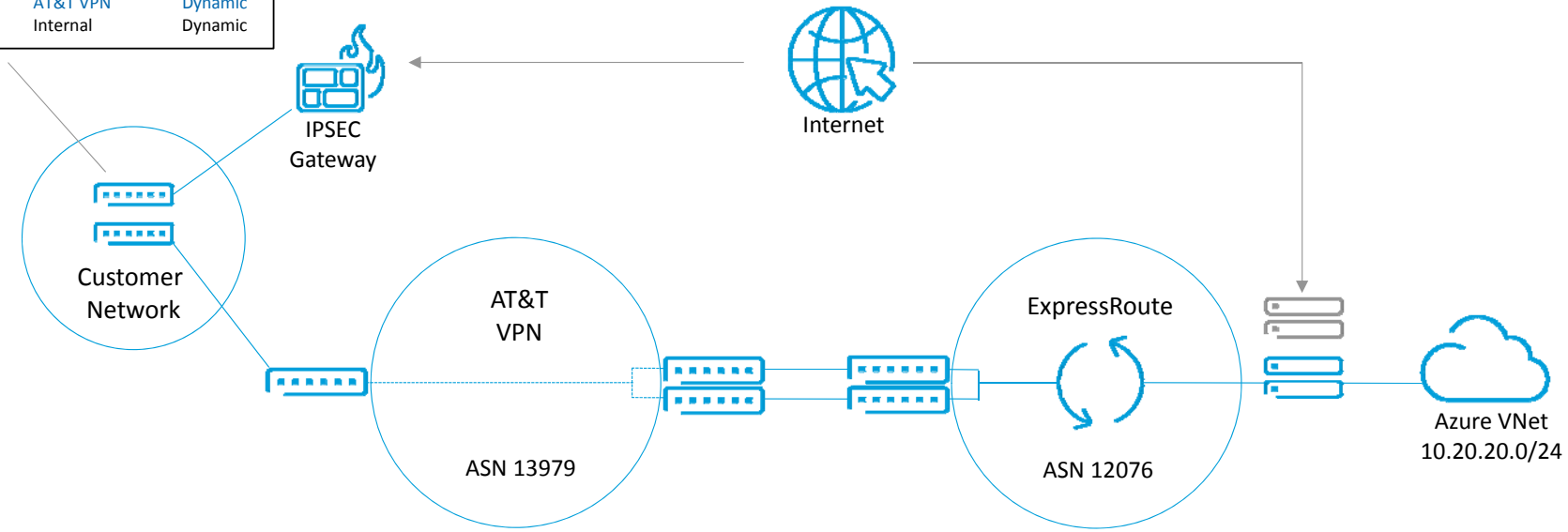
Route	Target	Routing
10.20.10.0/30	AT&T VPN	Dynamic
10.20.10.4/30	AT&T VPN	Dynamic
10.20.20.0/24	**Firewall**	**Static**
172.16.0.0/24	Internal	Dynamic



When migrating from a site-to-site VPN tunnel to NetBond for Cloud, first establish NetBond for Cloud connectivity with the Microsoft ExpressRoute circuit.

Migrating from Site to Site VPN Tunnels to NetBond (cont.)

Route	Target	Routing
10.20.10.0/30	AT&T VPN	Dynamic
10.20.10.4/30	AT&T VPN	Dynamic
~~10.20.20.0/24~~	~~Firewall~~	~~Static~~
10.20.20.0/24	AT&T VPN	Dynamic
172.16.0.0/24	Internal	Dynamic



During the migration maintenance window, delete the existing virtual network gateway and attach a new virtual network gateway to the virtual network. (This action can take up to 45 minutes to complete.) Then link the new VNet gateway to the Microsoft ExpressRoute.

Remove any static routes that were configured at the premise that routed traffic to Microsoft Azure via the VPN gateway.

VNC Itemized Billing

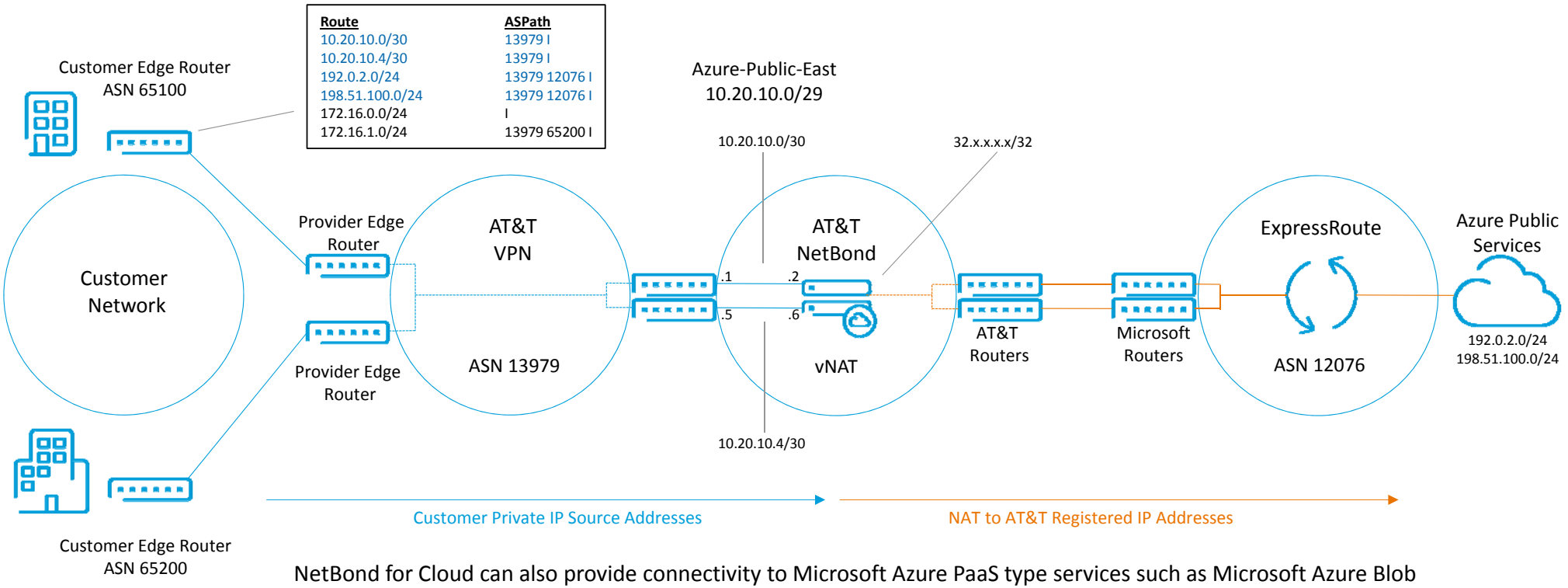
If a customer requires internal cost allocation they will need to establish individual service groups during initial VNC creation. This will provide itemized billing on the invoice.

Considerations

- Users that need access to all service groups should be configured as enterprise managers.
- Usage Notification Alerts are per service group.
- Portal Reporting is per service group.
- NetBond for Cloud features that are in controlled introduction will require an AT&T Cloud Solutions portal trouble ticket. You will need to create the service group first so that AT&T can complete the service ticket request.
- After a VNC is created under one service group, it cannot be migrated to another service group. It must be rebuilt in the new service group which will result in downtime.

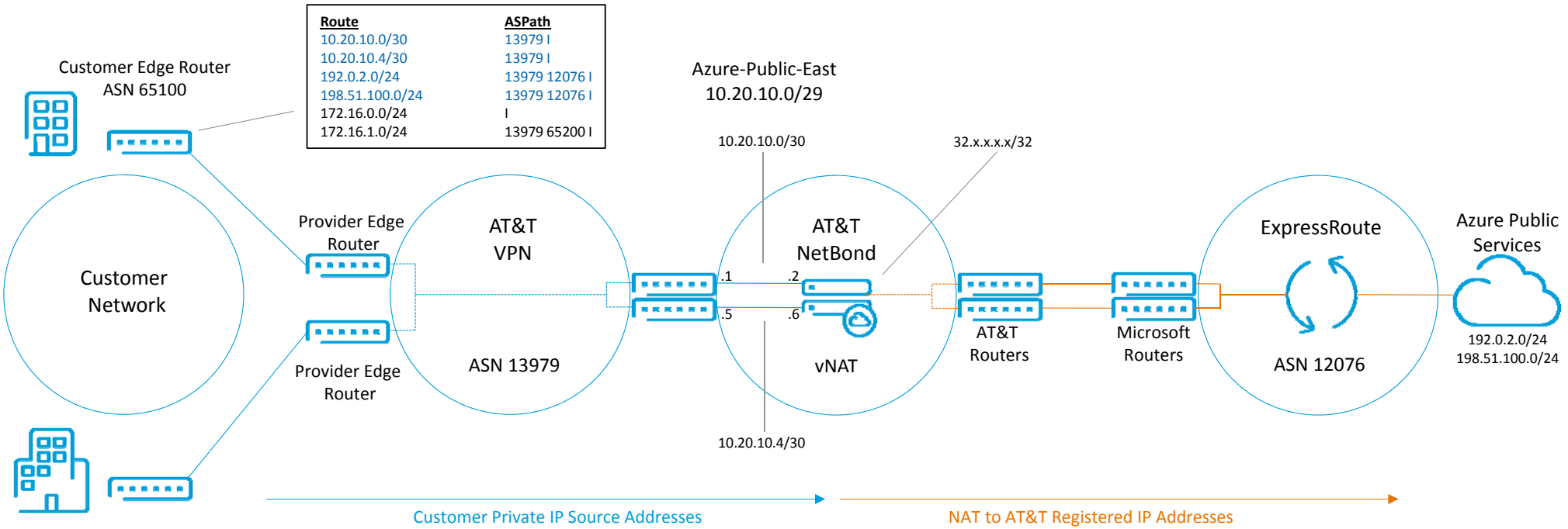
Service Activation Overview for Microsoft Azure Public Services

Public Services



NetBond for Cloud can also provide connectivity to Microsoft Azure PaaS type services such as Microsoft Azure Blob storage or Microsoft Azure Site Recovery. Since these services run in the Microsoft Azure public IP space, AT&T will provision a virtual network address translation device, to translate the customer's enterprise IP space to an AT&T registered public IP address. All of the Microsoft Azure public routes are advertised into the customer's enterprise routing tables. (Microsoft Office 365 routes are not included in public peering)

Public Services (cont.)



In our example, our customer creates a VNC, using the “Public” routing domain. Next a VLAN is created with a new /29 address space and the Microsoft ExpressRoute service key. (The same Microsoft ExpressRoute used for private peering can be shared for public peering.) Microsoft has preapproved all AT&T registered public IP addresses, so connectivity will come up immediately. All Microsoft subnets used for Microsoft Azure public services will be advertised to the customer’s MPLS VPN.

One consideration customers should take into account is that the enterprise will forward traffic for all Microsoft Azure public services via NetBond for Cloud. Thus, if any host on the network is conducting a transaction with a third party who happens to use Microsoft Azure public IP space as an underpinning to their website or service, then that transaction will occur over NetBond for Cloud.

What's Next?

What's Next After Activation? Confirming Connectivity

1. For the first connection to Microsoft Azure, schedule an activation call with the NetBond onboarding team.
2. After successfully creating your VNC and VLAN, we want to confirm basic network connectivity to Microsoft Azure.
3. After basic connectivity is confirmed, we ask that you take the following 5 business days to test your applications over NetBond for Cloud. Our client technical lead, is available to assist during this time if you have any questions or concerns, and they can be reached at DL-NetBondTeam@att.com.
4. After 5 business days, our cloud support team is available 24/7 to provide technical support and answer any questions. In addition, if you run into an emergency over these next 5 days, open a ticket in the AT&T Cloud Solutions portal to engage our cloud support team.

AT&T NetBond for Cloud Service Activation Overview for Microsoft Azure