Previous Unit 5 of 6 Next

200 XP

Knowledge check

13 minutes

When you consider a move to the cloud, it's essential in your role as an Azure developer, solution architect, or administrator that you know the fundamentals of how your network works. The next step in understanding the composition of a network is to take a detailed look at the interoperability of your network. This knowledge applies whether it's your organization's network, or more extensive networks like the web. All networks are built on the same principles.

In this unit, we examine the main aspects of network communications and why networks are built by using the Transmission Control Protocol/Internet Protocol (TCP/IP). Then, we discuss the differences between Internet Protocol address standards. Finally, we explore subnetting, the Domain Name System (DNS), ports, and the use and role of private IP addresses.

What is the Address Resolution Protocol?

The Address Resolution Protocol (ARP) is a communications protocol within the Internet Protocol suite. It's a request-response protocol used to resolve the media access control (MAC) address for a given IP address. ARP supports many data link layer technologies, such as Internet Protocol version 4 (IPv4), DECnet, and PUP. When an Internet Protocol version 6 (IPv6) address is resolved, the Neighbor Discovery Protocol (NDP) is used instead of ARP. Without ARP, there would be no means to resolve an IP address to a physical device address.

There's also the Reverse Address Resolution Protocol (RARP), which retrieves an IP address based on the given MAC address.

What is TCP/IP?

The Transmission Control Protocol/Internet Protocol is a collection of different communication protocols that support and define how network-enabled devices interconnect with each other over an IP-based network. At its heart are two key protocols: TCP and IP. TCP/IP makes the internet possible, including private and public networks, such as intranets and extranets.

TCP/IP defines the way data is shared between network-enabled devices by defining the end-to-end communication process. It manages how the message is broken down into packets of data, which are sometimes known as datagrams. TCP/IP also determines how the packet is addressed and transmitted, routed, and received. TCP/IP can determine the most efficient route across a network.

The TCP/IP model is designed to be stateless. This design means the network stack treats each request as new because it isn't related to the previous request. However, one part of the TCP/IP model isn't stateless. The transport layer operates in a stateful mode because it maintains a connection until all the packets in the message are received.

TCP/IP is an open standard. TCP/IP is governed, but no single organization owns it, so it works with all operating systems, networks, and hardware.

TCP/IP model layers

The TCP/IP model is made up of four distinct layers. Each layer uses a different type of protocol. Notice how the TCP/IP model is similar to the Internet Protocol suite discussed earlier.

- **Application layer**: The application layer determines which communication protocols are used. This layer includes HyperText Transfer Protocol (HTTP), DNS, File Transfer Protocol (FTP), Internet Message Access Protocol (IMAP), Lightweight Directory Access Protocol (LDAP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), Secure Shell (SSH), Telnet, and TLS/SSL.
- **Transport layer**: This layer splits the application data into manageable ordered chunks by using the right port for the application protocol used. The protocols associated with this layer are TCP and the User Datagram Protocol (UDP).
- **Internet layer**: Also called the network layer, this layer ensures the data packet gets to its destination. The protocols associated with this layer are IP, IPv4, IPv6, Internet Control Message Protocol (ICMP), and Internet Protocol Security (IPsec).
- **Network access layer**: This layer is responsible for defining how the data is sent across the network. The protocols associated with this layer are ARP, MAC, Ethernet, digital subscriber line (DSL), and Integrated Services Digital Network (ISDN).

What are the Internet Protocol standards?

Recall from earlier that the Internet Protocol isn't concerned about the order in which the packets are sent or received. It also doesn't guarantee a packet's delivery. The Internet Protocol only provides a logical addressing system that's used to route and forward messages to their destinations.

Today, there are two Internet Protocol versions that work within networks: IPv4 and IPv6.

IPv4

Internet Protocol version 4 was released in 1983, and is the standard for all packet-switch-based networks in use today. IPv4 uses a 32-bit address space that gives an upper limit of 4,294,967,296 (4.3 billion) unique logical IP addresses. A large number of these available IP addresses are reserved for a specific purpose, such as private networks, local hosts, internet relays, documentation, and subnets.

Structure of an IPv4 address

The structure of an IPv4 address is four decimal numbers in the range of 0 to 255, each separated with a dot. This structure is also known as the dotted-decimal format. An example of an IP address is 192.168.0.1.

Parts of an IPv4 address

There are two parts to an IP address, the network and the host. Let's use the address `192.168.0.1` as an example.

The network part of an IP address covers the first set of decimal numbers. In the example, that's `192.168.0`. This number is unique to the network and specifies the class of the network. There are many network classes available, as described in the following section.

The host part of the IP address covers the next set of decimal numbers. In the example, that's `1`. This number represents the device and must be unique within the network to avoid address conflicts. Each device on a network segment must have a unique address.

IPv4 address classes

The Internet Protocol's local address space is split into five logical classes or ranges of IP addresses, each represented by a letter of the alphabet.

Expand table

Class	Start address	End address	Number of networks	IP addresses per network	Total IP addresses available	Subnet mask
A	0.0.0.0	127.255.255.255	128	16,777,216	2,147,483,648	255.0.0.0
B	128.0.0.0	191.255.255.255	16,384	65,536	1,073,741,824	255.255.0.0
C	192.0.0.0	223.255.255.255	2,097,152	256	536,870,912	255.255.255.0
D	224.0.0.0	239.255.255.255	-	-	268,435,456	-
E	240.0.0.0	255.255.255.255	-	-	268,435,456	-

For classes A, B, and C, the start and end IP addresses are reserved and shouldn't be used. Class D is reserved for multicast traffic only. Class E is reserved and can't be used on public networks like the internet.

In the previous table, the last column is marked as a subnet mask. The subnet mask uses the same format as the IP address, but its purpose is to identify valid IP addresses in an IP range.

For example, assume you have an IP address range that starts at `192.168.0.1`, and you have a subnet of `255.255.255.0`. You apply the subnet mask in the following way. For each address segment value specified as 255 in the mask, the corresponding address segment is static. When you want to pick an IP address, you must pick an address that matches `192.168.0`. Where the segment has a value of `0`, you can use any value between 0 to 255. A subnet mask of `255.255.255.0` gives an IP address range of `192.168.0.0` to `192.168.0.255`, which are valid values to select.

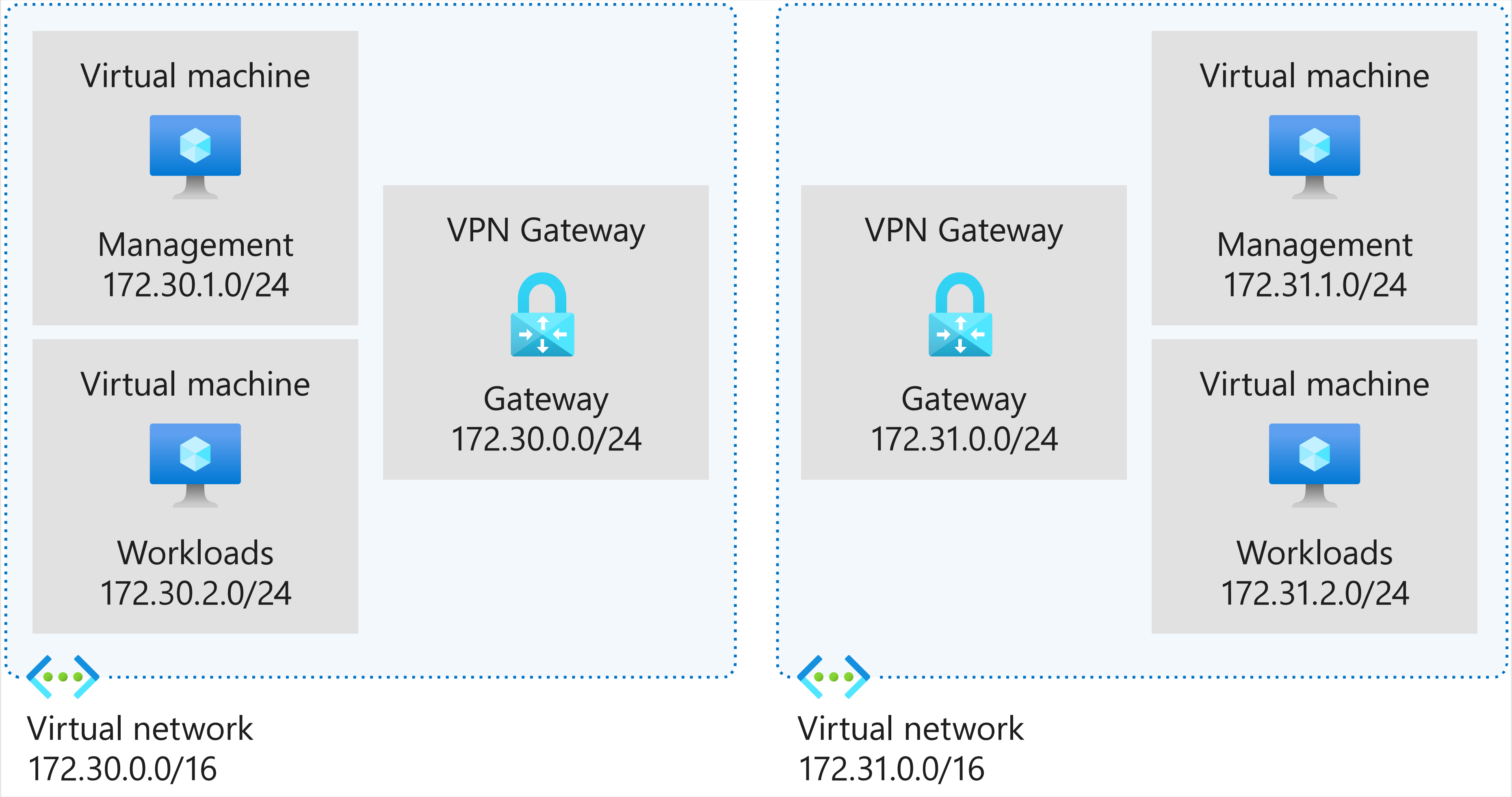
What is a subnet?

A subnet defines one or more logical networks within the class A, B, or C network. Without subnets, you can only have a single network in each of the class A, B, or C networks.

An IP address, also known as a network address or routing prefix, represents the address of the device or computer to send the packet of data. A subnet, or host address, represents which network or subnetwork to use. A subnet is a 32-bit number framed by using the dotted-decimal format. For example, 255.255.255.0 is a standard subnet mask.

In an IPv4 network, for a packet of data to be routed to the correct network and network device, a routing prefix is needed. A routing prefix is created by taking the subnet mask and applying a bitwise `AND` to the IP address.

A more common way to define the subnet and the routing prefix is to use the Classless Interdomain Routing (CIDR) notation. CIDR applies to the IP address as the number of bits you want to allocate to your subnet. Using CIDR notation, at the end of the IP address, add a "/" and then the number of bits. For example, 198.51.100.0/24 is the same as using the dotted-decimal format subnet mask 255.255.255.0. It offers an address range of 198.51.100.0 to 198.51.100.255.



Subnets allow multiple subnetworks to exist within one network. They can be used to enhance routing performance. Subnets can be arranged hierarchically to create routing trees.

Special-use addresses

Each of the classes has restrictions on the ranges of IP addresses that can be used. This table shows the more common ones.

⛶ Expand table

Address range	Scope	Description
10.0.0.0–10.255.255.255	Private network	Used for local communications within a private network
127.0.0.0–127.255.255.255	Host	Used for loopback addresses
172.16.0.0–172.31.255.255	Private network	Used for local communications within a private network
192.88.99.0–192.88.99.255	Internet	Reserved
192.168.0.0–192.168.255.255	Private network	Used for local communications within a private network
255.255.255.255	Subnet	Reserved for the "limited broadcast" destination address

IPv4 address space exhaustion

Soon after the introduction of IPv4, it became apparent that the pool of available IP addresses was being consumed faster than was expected. For example, think about the number of mobile devices that were released in the last couple of years.

Several solutions were introduced to mitigate the threat of running out of IP addresses. These ideas included network address translation (NAT), classful networks, and CIDR. In the 1990s, IPv6 was created to increase the number of IP address spaces to 128 bits. IPv6 was introduced commercially in 2006.

Private IP addressing

In classes A, B, and C, a range of IP addresses are set aside for private networks. These IP ranges aren't accessible via the internet. All public routers ignore any packets sent to them containing such an address.

Expand table

Name	CIDR block	Address range	Number of addresses	Classful description
24-bit block	10.0.0.0/8	10.0.0.0–10.255.255.255	16,777,216	Single class A
20-bit block	172.16.0.0/12	172.16.0.0–172.31.255.255	1,048,576	Contiguous range of 16 class B blocks
16-bit block	192.168.0.0/16	192.168.0.0–192.168.255.255	65,536	Contiguous range of 256 class C blocks

Network devices on a private network can't communicate with devices on a public network. Communication can happen only through network address translation at a routing gateway.

The only way to connect two private networks in different geographical areas is to use a virtual private network (VPN). A VPN encapsulates each private network packet. The VPN can further encrypt the packet before it sends it across a public network from one private network to another private network.

IPv6

Internet Protocol version 6 is the latest version of the IP standard. The Internet Engineering Task Force (IETF), designed and developed IPv6 to address the problem of IPv4 logical address exhaustion. It was intended to eventually replace the IPv4 standard. It was adopted as a recognized internet standard in July 2017.

IPv6 uses a 128-bit address space, which allows 2^{128} addresses. This amount is approximately 7.9x10^{28} times more than IPv4.

IPv4 and IPv6 weren't designed to be interoperable, which slowed down the transition to the newer IPv6 standard.

IPv6 also introduced several benefits:

- **Simplified network configuration**: IPv6 has address autoconfiguration built into the protocol. For example, a router broadcasts the network prefix, and the network device can append its MAC address to self-assign a unique IPv6 address.
- **Security**: IPsec is built into IPv6.
- **New service support**: IPv6 eliminates the need for NAT, which makes it easier to create peer-to-peer networks.
- **Multicast and anycast functionality**: Multicast allows for the broadcast of messages in a one-to-many fashion. Anycast allows a single destination to have multiple routing paths to two or more endpoint destinations.

Structure of an IPv6 address

The structure of IPv6 is different from IPv4. Instead of four decimal numbers, it uses eight groups of four hexadecimal numbers called a hexadectet. Each hexadectet is separated with a colon. A full IPv6 address looks like this: `2001:0db8:0000:0000:0000:8a2e:0370:7334`.

The new standard allows for the address to be simplified by using the following rules:

- One or more leading zeros from any group can be removed, so `0042` becomes `42`.
- Consecutive sections of zeros are replaced with a double colon (`::`), which can be used only once in an address.

The shortened version of the IPv6 example is `2001:db8::8a2e:370:7334`. Notice that all the instances of `0000` are removed.

DNS

DNS is a decentralized lookup service that translates a human-readable domain name or URL into the IP address of the server that's hosting the site or service. The worldwide distributed nature of DNS is a vital component of the internet. DNS has been in use since its inception in 1985.

A DNS server serves two purposes. The first is to maintain a cache of recently searched-for domain names, which improves performance and reduces network traffic. The second is to act as the start of authority (SOA) for all the domains under it. When a DNS server is looking to resolve a domain name that isn't held in its cache, it starts with the highest level, the dot. It then works down the subdomains until it finds the DNS server acting as the SOA. Once found, it stores the IP address of the domain in its local cache.

The DNS also holds specific records that relate to the domain. These records include the SOA, IP addressing (A and AAAA), SMTP email (MX), name servers (NS), and domain name alias (CNAME) records.

What does Azure offer?

While many of the concepts discussed here are technical, Azure builds and extends several of these aspects with tools that can help with the configuration of your network.

Azure DNS

Azure DNS is a service for hosting registered domain names by using the Azure infrastructure. You can use Azure DNS to manage your DNS records. By using your regular Azure sign-in credentials, you can manage records such as A, AAAA, CNAME, SOA, NS, and MX.

One of the core benefits provided by Azure DNS is the alias record, which can use either an A, AAAA, or CNAME record. By using the alias, you can route traffic to an Azure resource.

Azure DNS doesn't replace domain registrars, where you register and purchase domains.

Azure Virtual Network

You can use Azure Virtual Network to build a private network in the cloud. With an Azure virtual network, you can build networks that can communicate with other virtual networks and your on-premises network. They're an efficient way to extend your network into the cloud.

With an Azure virtual network, you can control the addressing used. Most virtual networks are assumed to be private networks. As with a regular network, you can use subnetting to segment and give IP address ranges to those subnets.

Check your knowledge

1. What is the structure of an IPv4 address? *

○ It's made up of four groups of eight numbers, each separated by a dot.

○ It's made up of four hexadecimal numbers (0-F), each separated by a colon.

○ It's made up of four numbers, in the range 0-255, each separated by a dot.

2. What is TCP/IP? *

○ It's a protocol that improves network device security on the internet.

○ It's a protocol used to secure connections on the internet.

○ It's a protocol used to interconnect network devices on the internet.

3. What is a subnet? *

○ It's the natural subdivision of an IP address into host and network.

○ It's a control mechanism to limit access to an IP-based network.

○ It's the logical subdivision of an IP-based network.

4. How would you access a private network from the internet? *

○ By connecting directly to the IP address of the private network.

○ The private network needs special access via a gateway.

○ It's possible to access a private network from the internet. A private network can't access another private network by using network address translation.

5. What is the DNS? *

○ The DNS helps resolve IP addresses to domain names.

○ The DNS helps resolve MAC addresses to IP addresses.

○ The DNS helps resolve domain names to IP addresses.

Check your answers

Check your answers