**Networking and Kubernetes**

**ARP** stands for Address Resolution Protocol which is one of the most important protocols of the Data link layer in the OSI model. It is responsible to find the hardware address of a host from a known IP address.

**Multiplexing, or muxing**, is a way of sending multiple signals or streams of information over a communications link at the same time in the form of a single, complex signal.

An **Autonomous System Number** (AS number or just **ASN**) is a special number assigned by IANA used primarilly with Border Gateway Protocol which uniquely identifies an network under a single technical administration that has a unique routing policy, or is multi-homed to the public internet.

**Border Gateway Protocol (BGP)** is a set of rules that determine the best network routes for data transmission on the internet. The internet consists of thousands of private, public, corporate, and government networks linked together through standardized protocols, devices, and communication technologies.

A **netmask** is a mask used to divide an IP address into subnets and specify the number of available host addresses in the subnet.

A **genmask** is the [netmask](http://docs.intenogroup.com/v315/en/glossary/n/netmask) for the destination net.

For example 255.255.255.255 for a host destination and 0.0.0.0 for the default route

On transport protocols such as TCP, UDP, and SCTP,

**ports 1-1023** are by default **privileged ports**. To bind to a privileged port, a process must be running with root permissions.

Ports that are **greater than 1023** are by default **non-privileged.**

[**Kernel**](https://www.geeksforgeeks.org/kernel-i-o-subsystem-in-operating-system/) is central component of an operating system that manages operations of computer and hardware.

It basically manages operations of memory and CPU time.

It is core component of an operating system.

Kernel **acts as a bridge** between applications and data processing performed at hardware level using inter-process communication and system calls.

A ***network interface*** is the point of interconnection between a computer and a private or public network.

A network interface is generally a network interface card (NIC), but does not have to have a physical form.

Instead, the network interface can be implemented in software.

For example, the loopback interface (127.0.0.1 for IPv4 and ::1 for IPv6) is not a physical device but a piece of software simulating a network interface. The loopback interface is commonly used in test environments.

A **hook** is a location in the kernel that + calls out of the kernel to a kernel module routine - a hook exit routine

The **MASQUERADE target** is used basically the same as the SNAT target, but it does not require any --to-source option. The reason for this is that the MASQUERADE target was made to work with, for example, dial-up connections, or DHCP connections, which gets dynamic IP addresses when connecting to the network in question. This means that you should only use the MASQUERADE target with dynamically assigned IP connections, which we don't know the actual address of at all times. If you have a static IP connection, you should instead use the SNAT target.

**Cheat sheet of common debugging cases and tools**

Checking connectivity -> **traceroute, ping, telnet, netcat**

Port scanning ->  **nmap**

Checking DNS records-> **dig**, commands mentioned in “Checking Connectivity”

Checking HTTP/1 -> **cURL, telnet, netcat**

Checking HTTPS -> **OpenSSL, cURL**

Checking listening programs-> **netstat**

**Libnetwork** provides a native Go implementation for connecting containers.

The goal of libnetwork is to deliver a robust Container Network Model that provides a consistent programming interface and the required network abstractions for applications.

## What is an RFC1918 address?

An [RFC1918](https://tools.ietf.org/html/rfc1918) address is an IP address that is assigned by an enterprise organization to an internal host. These IP addresses are used in [private networks](https://en.wikipedia.org/wiki/Private_network), which are not available, or reachable, from the Internet.

In fact, one of the basic requirements of the Internet is that each host has a unique IP address. RFC1918 removes this requirement. RFC1918 IP addresses can be used on multiple networks, as long as they’re private and isolated from each other. To implement this solution every Internet router must be configured to discard IP packets with these addresses. IP packets carrying private addresses can only flow on internal, private networks. This aspect contributes to network security by creating a clear distinction between internal and external networks. Devices with private addresses are not directly reachable from the Internet, which adds a layer of isolation and protection against certain types of cyber threats.

**kubectl port-forward** forwards connections to a local port to a port on a pod

**Deployment + Service in Kubernetes [ using YAML ]**

**Link:**

https://medium.com/@SabujJanaCodes/building-a-golang-music-api-and-deploying-it-on-k8s-go-mysql-k8s-841612d13479