UNIX NETWORKING

Architecture & Deployment

Speaker notes

Learn the basics of Unix networking and how to make TCP connections.

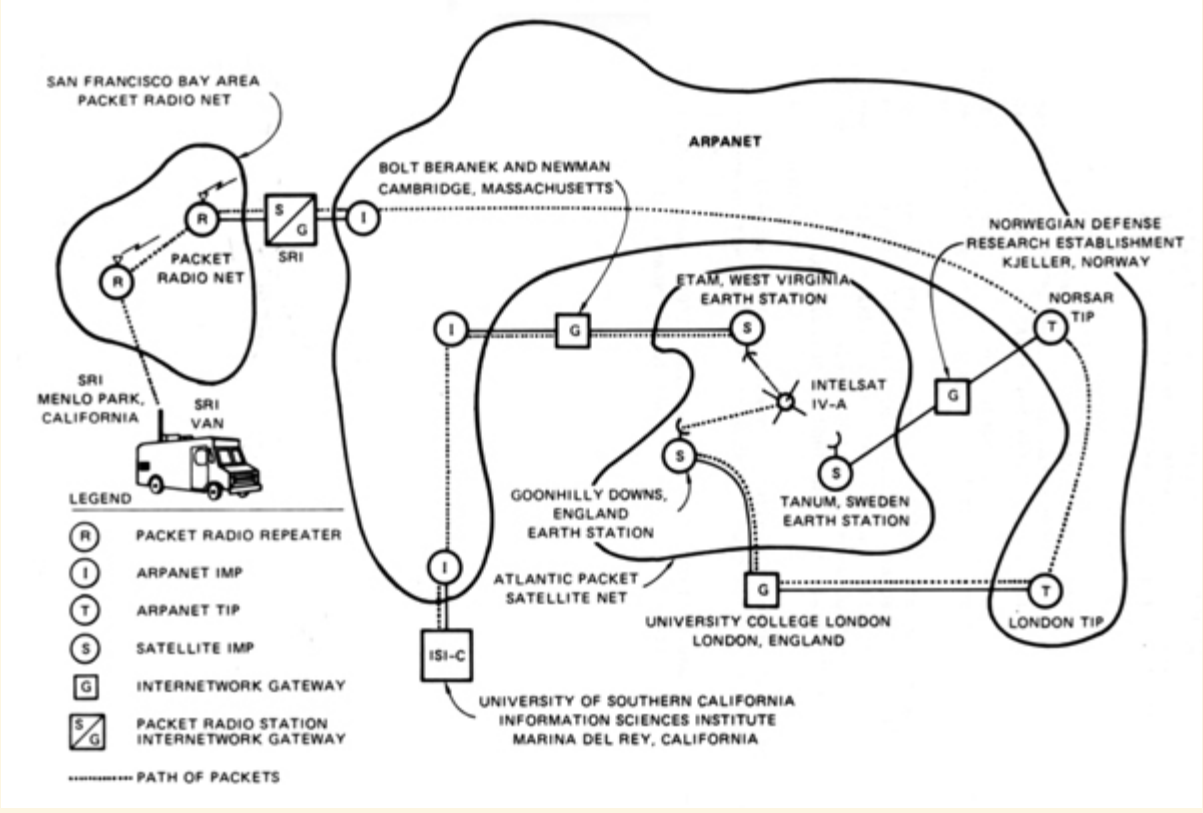
You will need

- A Unix CLI
- An Ubuntu server with a public IP address to connect to

Recommended reading

- Unix Basics & Administration
- Unix Processes

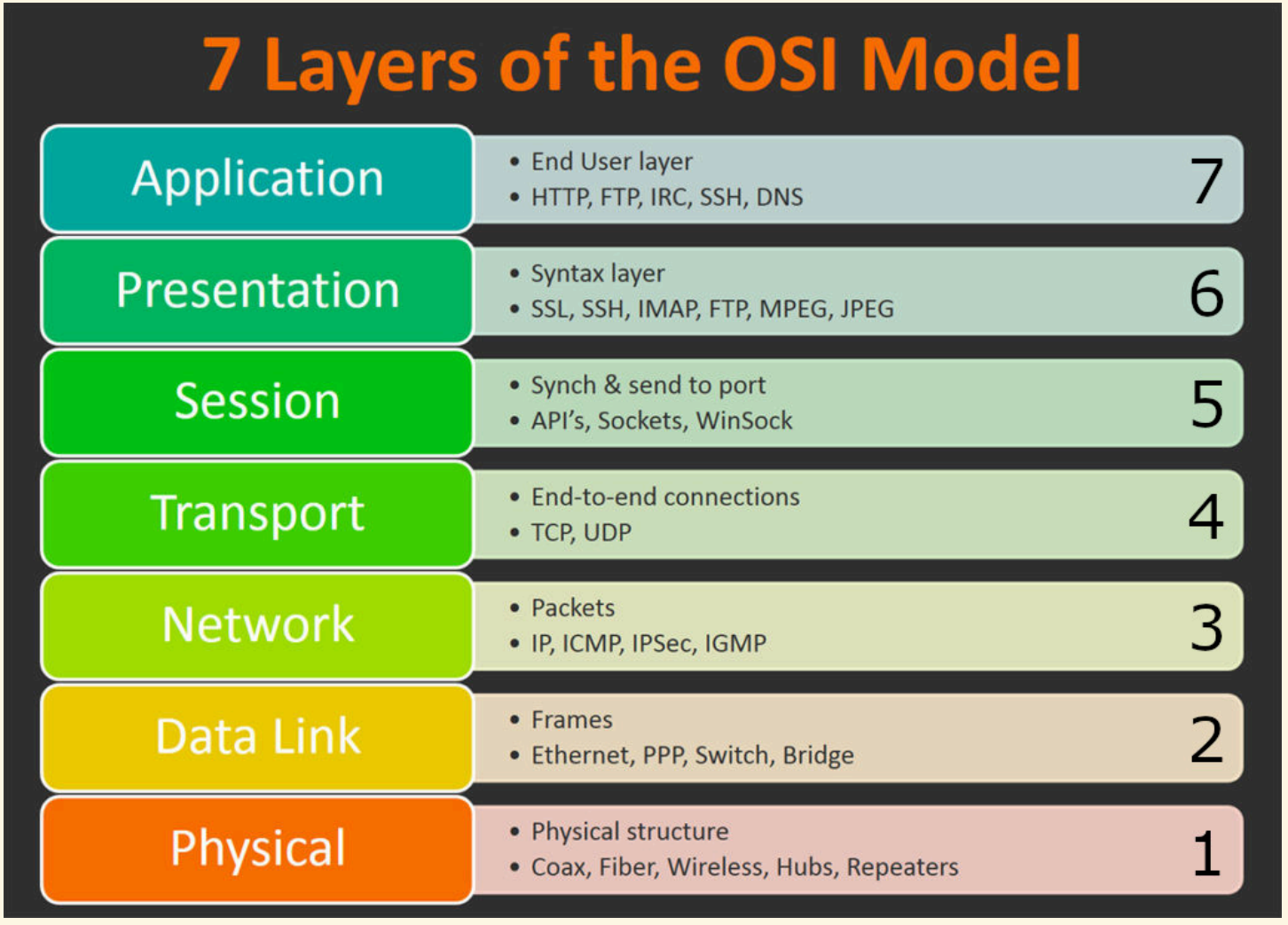
MEANWHILE IN 1977



Speaker notes

This is a diagram of the first internetworked TCP connection made between sites in the US, the UK and Norway in 1977.

7 Layers of the OSI Model

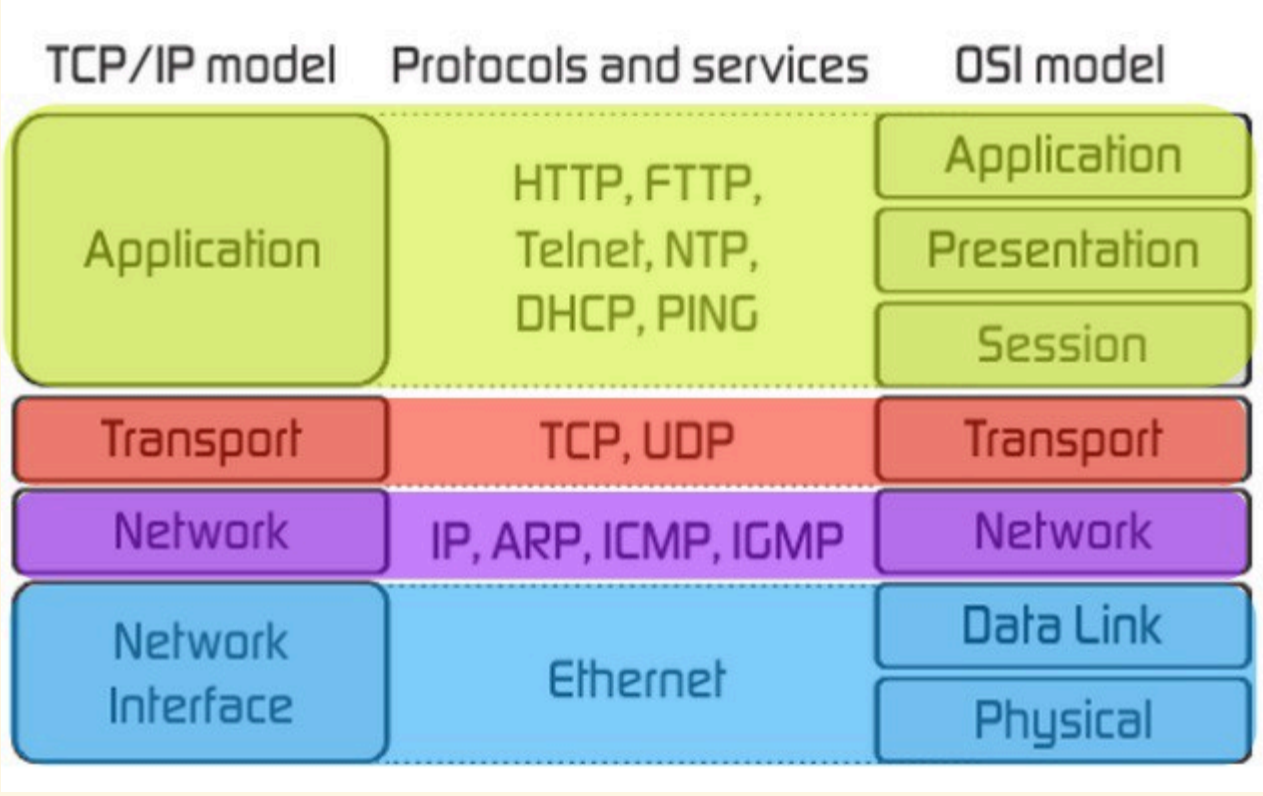


Speaker notes

The **O**pen **S**ystems **I**nterconnection (OSI) model standardizes communications between computing systems, allowing interoperability with standard protocols.

A layer serves the layer above it and is served by the layer below it.

OSI VS. TCP/IP MODEL



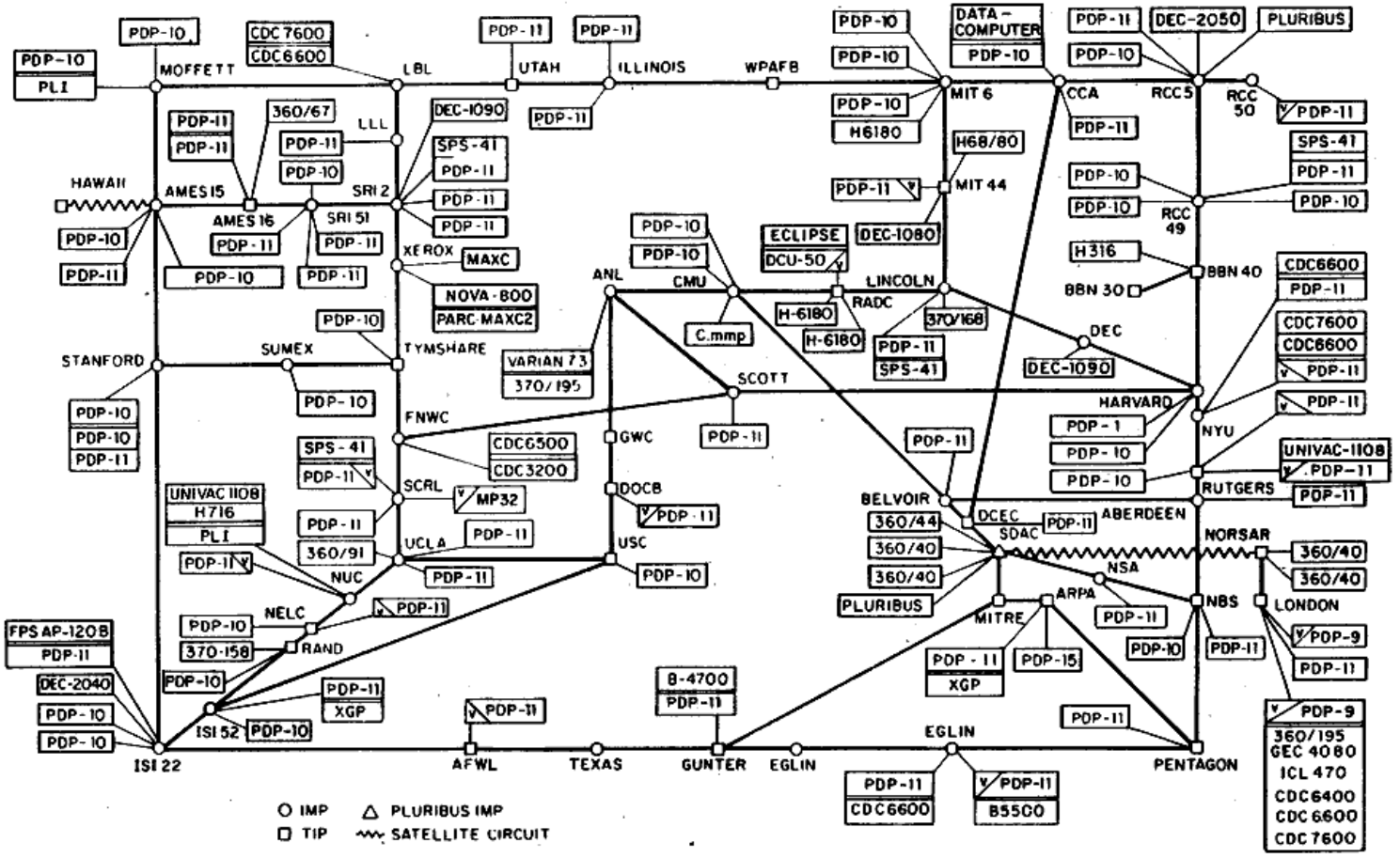
Speaker notes

The Internet protocol suite is the conceptual model used on the Internet and on similar computer networks. It is commonly known as TCP/IP since the **T**ransmission **C**ontrol **P**rotocol (TCP) and the **I**nternet **P**rotocol (IP) are its foundational protocols.

It was originally developed for ARPANET.

The OSI and TCP/IP models describe the same technologies, but categorize them a little differently. The OSI model is used more as a theoretical construct to reason about networking systems, while the TCP/IP model is more in line with how Internet protocols are designed and used in practice.

ARPANET LOGICAL MAP, MARCH 1977



(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

THE INTERNET PROTOCOL (IP)

- Deliver packets from source to destination
- **Network layer** protocol (OSI layer 3)

Speaker notes

The **I**nternet **P**rotocol (IP) is the principal communications protocol of the Internet. It allows delivering packets from a source host to a destination host based solely on IP addresses. It is a **network layer** protocol (OSI layer 3).

IPv4

- In use since 1983
- 32-bit address space (~4 billion addresses)
- Decimal notation for humans

172	.	16	.	254	.	1
10101100		00010000		11111110		00000001

Speaker notes

Version **4** of the protocol (**IPv4**), in use since 1983, uses a 32-bit address space, meaning that there are 2^{32} or about 4.3 billion possible addresses.

Of course 32 bits are a little hard to remember or even write down, so an IPv4 address is typically represented in 4 dotted decimal notation, with each octet (8 bits) containing a value between 0 and 255 (i.e. 2^8 possibilities).

IPv6

- In use since 2017
- 128-bit address space (a lot)
- Hexadecimal notation for humans

2001	.	0db8	.	85a3	.	0000	.	0000	.	8a2e	.	0370	.	7334
00100000		00001101		10000101		00000000		00000000		10001010		00000011		01110011
00000001		10111000		10100011		00000000		00000000		00101110		01110000		00110100

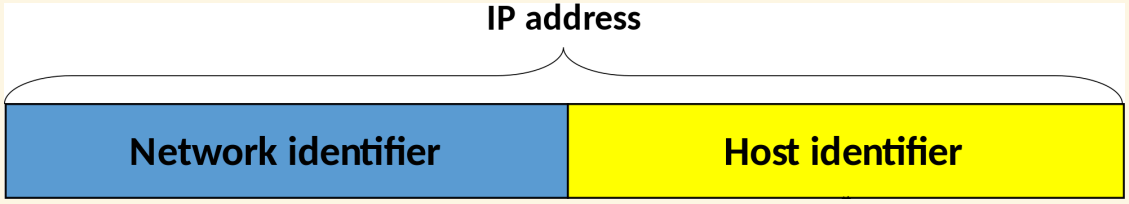
Speaker notes

Version **6** of the protocol (**IPv6**) was developed more recently because the world is running out of IPv4 addresses (~4 billion IPv4 addresses is not enough in the Internet of Things (IoT) world). It's an Internet standard since 2017.

IPv6 adresses are typically represented as 8 groups of 4 hexadecimal digits. Here's the same address in hexadecimal format: `0123:4567:89ab:cdef:0123:4567:89ab:cdef`

2^{128} possibilities is about 340 undecillion (yes, that's a word) addresses, or 3.4 with 38 zeros. At least we won't have a year 2038 bug.

IP NETWORKS



172 . 16 . 254 . 1

Speaker notes

Each computer that is publicly accessible on the Internet has a **public IP address**. To facilite routing, IP addresses are logically divided into networks.

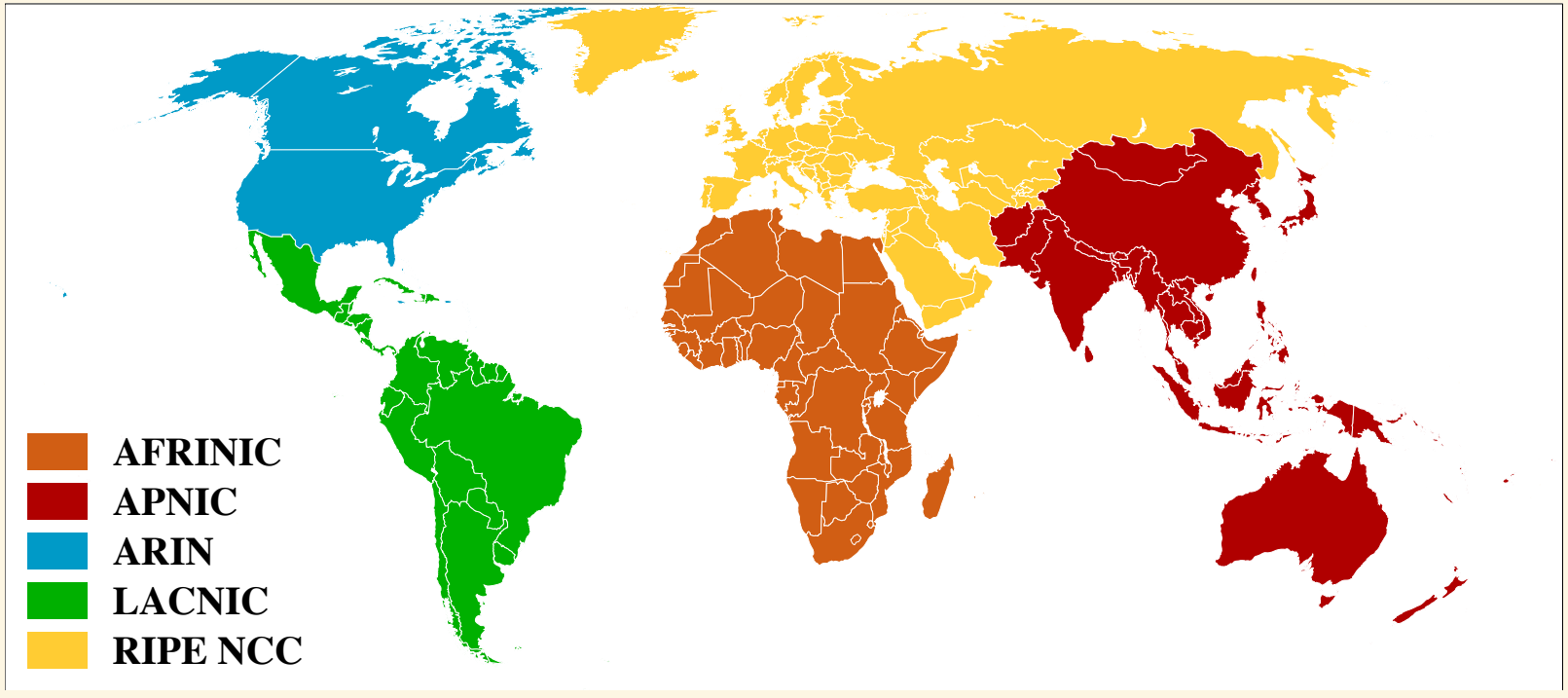
For example, assuming we use the address `10101100000100001111111000000001`, or `172.16.254.1` in dotted decimal notation, and a prefix of 16 bits:

- The **network identifier or prefix** would be the first 16 bits: `1010110000010000`, or in decimal notation `172.16`
- The **host identifier** would be the last 16 bits: `1111111000000001` or in decimal notation `254.1`

This allows the physical routing devices that are part of the Internet to direct traffic to the correct geographical area and machine(s).

IP GLOBAL NETWORKS

Regional **I**nternet **R**egistries (RIR): IPv4 Registry, IPv6 Registry, managed by **I**nternet **A**ssigned **N**umbers **A**uthority (IANA)



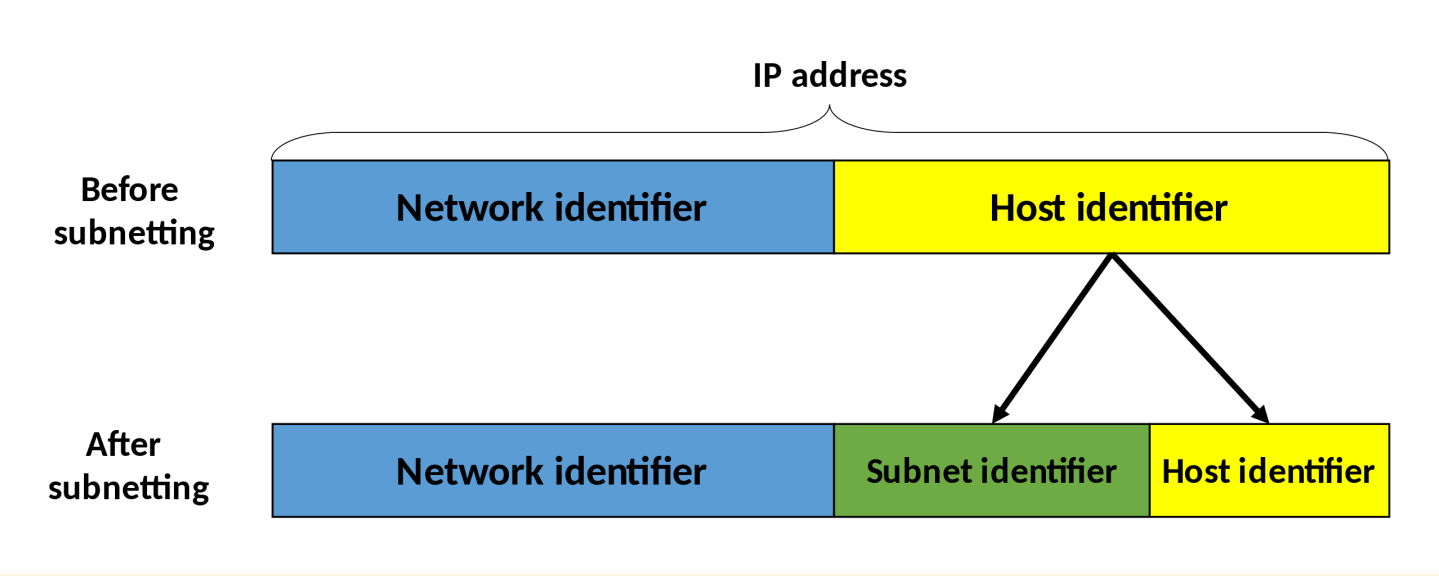
Speaker notes

The **I**nternet **A**ssigned **N**umbers **A**uthority (IANA) is the organization responsible for dividing the Internet itself into global networks, each administered by regional organizations.

The **R**egional **I**nternet **R**egistries (RIR), in turn, follow their regional policies to delegate resources to their customers, which include **I**nternet **S**ervice **P**roviders (ISP) (e.g. Swisscom).

You can find the list of registered networks in the IPv4 Address Space Registry and IPv6 Address Space Registry.

IP LOCAL NETWORKS



172 . 16 . 254 . 1

Speaker notes

Subnetting can be used to further improve efficiency in the utilization of the relatively small address space available.

Instead of having thousands of computers in the same network all able to directly contact each other, subnetting allows organizations to create smaller, isolated networks with fewer computers.

This can be used to define **complex network structures** within an organization or to **improve security**.

NETMASKS AND CIDRS

IP address	172	.	16	.	254	.	1
	10101100		00010000		11111110		00000001
Netmask	255	.	255	.	0	.	0
	11111111		11111111		00000000		00000000
CIDR	/16						

Speaker notes

A netmask is a notation to define an IPv4 network. Let's take the example of a random address `172.16.254.1` in the third private address range with the netmask `255.255.0.0`.

Look at the netmask in binary form. The leading `1`s indicate the bits used for the network prefix and the trailing `0`s indicate the bits used for the host identifier. A netmask is always a sequence of `1`s followed by a sequence of `0`s.

CIDR is another more compact notation that expresses the same thing. Writing `172.16.254.1/16` means that the first 16 bits of the address are used as the network prefix. It is therefore equivalent to `172.16.254.1` with the netmask of `255.255.0.0`. Similarly, `10.0.0.0/8` is equivalent to `10.0.0.0` with a netmask of `255.0.0.0` (i.e. the first 8 bits are the network prefix).

MORE NETMASKS AND CIDRS

IP address	172	.	16	.	254	.	1
	10101100		00010000		11111110		00000001
Netmask	255	.	0	.	0	.	0
	11111111		00000000		00000000		00000000
CIDR	/8						

RESERVED ADDRESSES FOR PRIVATE NETWORKS

First address	Last address	Netmask	CIDR	Addresses
`10.0.0.0`	`10.255.255.255`	`255.0.0.0`	`/8`	2^{24} ~16 million
`172.16.0.0`	`172.31.255.255`	`255.240.0.0`	`/12`	2^{20} ~1 million
`192.168.0.0`	`192.168.255.255`	`255.255.0.0`	`/16`	2^{16} 65,536

Speaker notes

There are a few reserved IP address ranges. Some are **reserved for private networks**. In these ranges you **cannot communicate with public machines** without a NAT gateway or proxy.

There are three reserved private ranges in the IPv4 address space.

RESERVED RANGE FOR LOOPBACK ADDRESSES

First address	Last address	Netmask	CIDR	Addresses
`127.0.0.0`	`127.255.255.255`	`255.0.0.0`	`/8`	2^{24} ~16 million

Speaker notes

Additionally, the following range is **reserved for a virtual network interface**, allowing networking applications running on the same machine to communicate with one another.

THERE'S NO PLACE LIKE 127.0.0.1

These addresses all resolve to the current computer, bypassing network hardware.

Hostname	`localhost`
IPv4 address	`127.0.0.1`
IPv6 address	`::1`

Speaker notes

`localhost` is a hostname that refers to the current computer used to access it. It normally resolves to the IPv4 loopback address `127.0.0.1`, and to the IPv6 loopback address `::1`.

When you or a program makes a request to `localhost` or `127.0.0.1`, you are contacting your own computer, bypassing network hardware but otherwise behaving the same way as any other network call.

NOT AN IP ADDRESS

`0.0.0.0`

This generally means "any IP address".

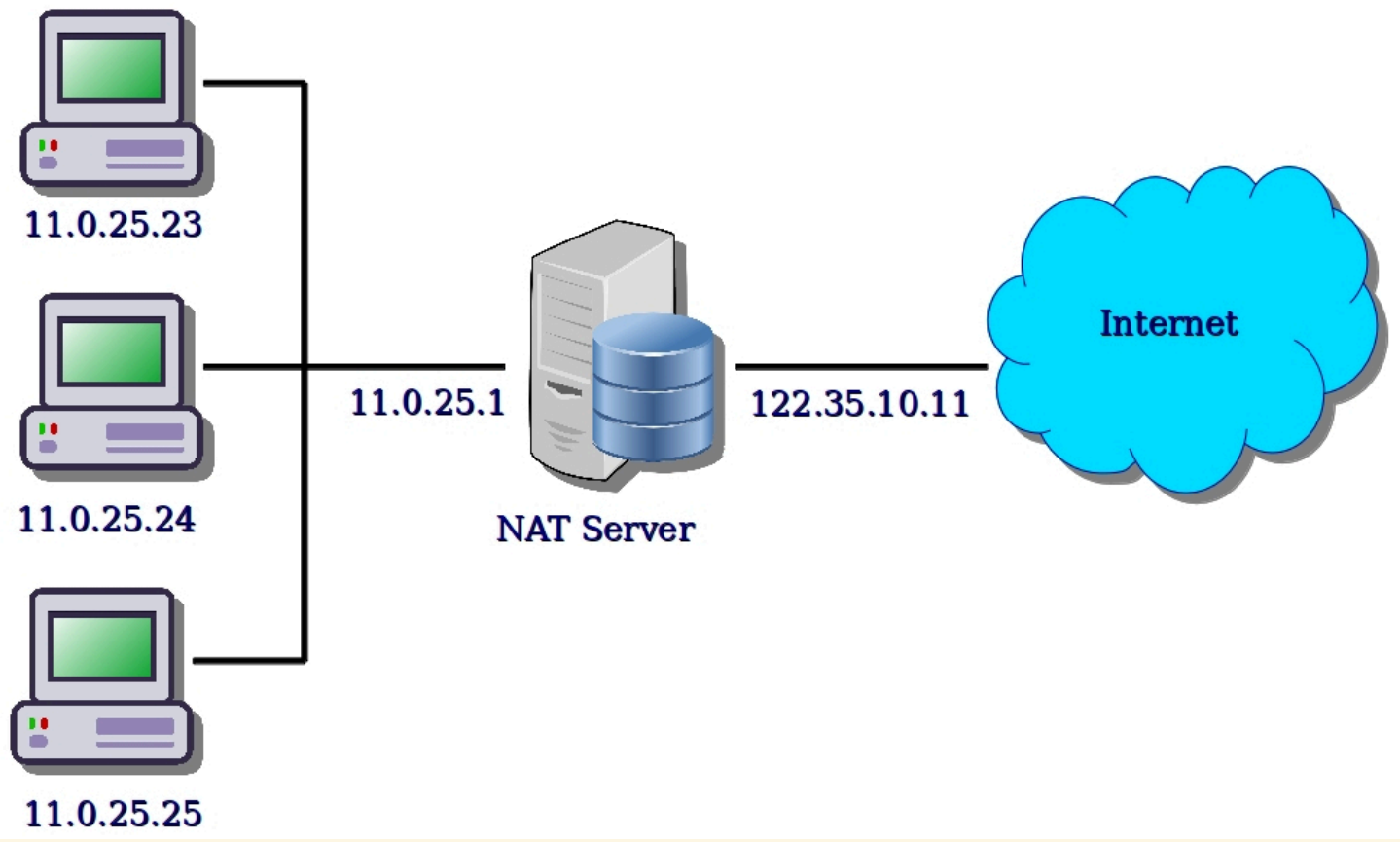
Speaker notes

You will sometimes encounter `0.0.0.0`. This is not an actual IP address.

One computer can have several IP addresses. Processes that listen for incoming requests (e.g. a database or a web server) generally allow you to **restrict which IP address they can be reached on**. You may only want to accept requests to one specific address.

When you want to allow anyone to reach the process on any IP address the computer may have, you can sometimes use `0.0.0.0` as a special notation that means "**all IP addresses on the local machine**". The IPv6 equivalent is `::`.

NETWORK ADDRESS TRANSLATION (NAT)



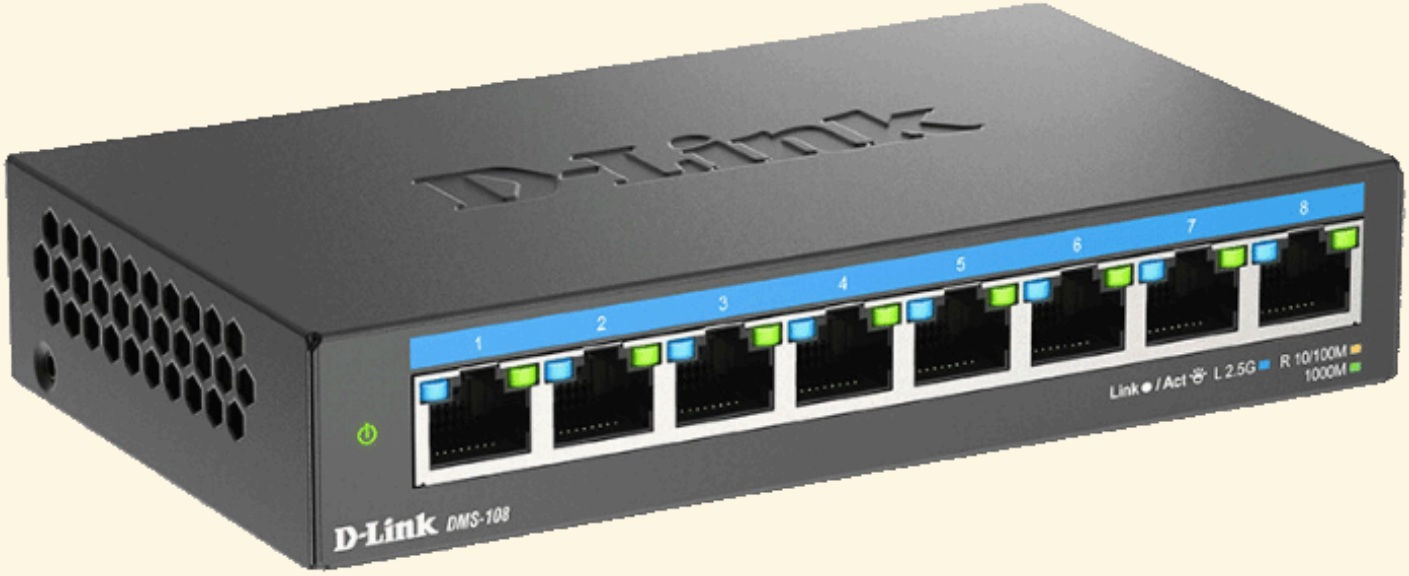
Speaker notes

Network **A**ddress **T**ranslation (NAT) is a method of **remapping one IP address space into another** as traffic goes through a routing device.

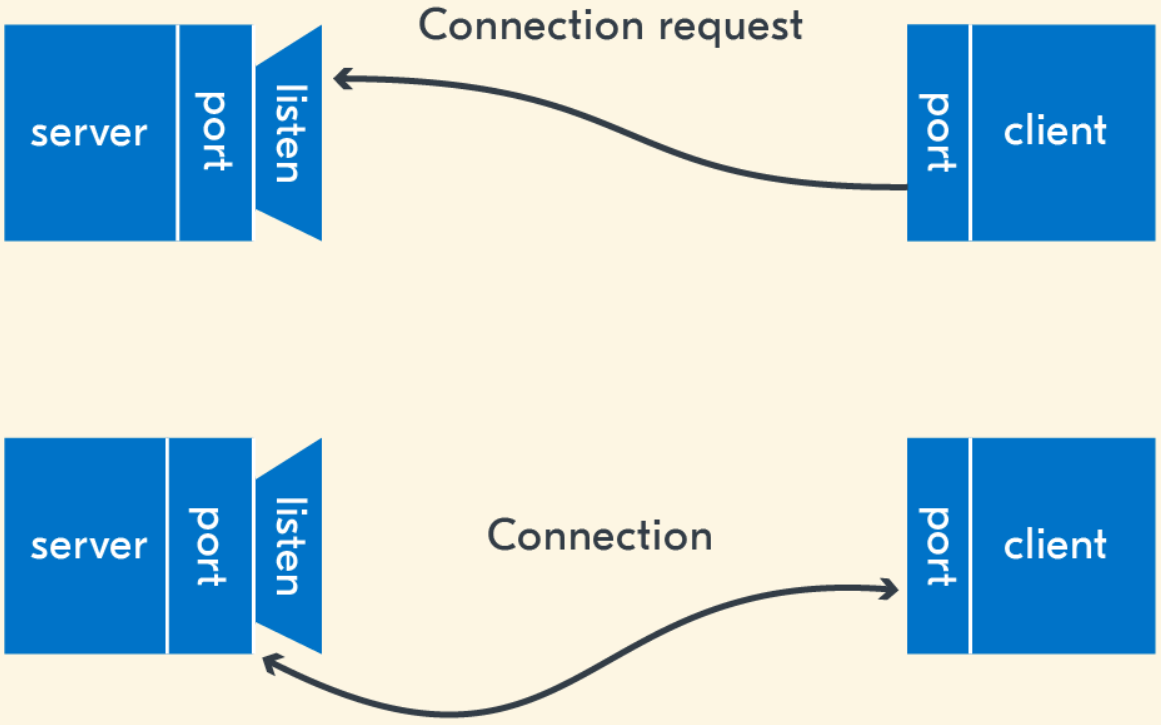
It is very commonly used for **IP masquerading**, a technique that hides an entire IP address range (such as private IP addresses) behind a single public IP address. The router typically translates the private IP addresses of computers in an organization's network into a single public IP address assigned to the organization and vice-versa.

Other computers on the Internet see the traffic as originating from the routing device with the public IP address instead of the hidden computer in the private network. This technique helps conserve IPv4 address space.

PORTS



NETWORK PORTS



WHAT'S A NETWORK PORT?

- 16-bit number: from 0 to 65,535
- Associated to an IP address when communicating
- **Transport layer** protocols (OSI layer 4):
  - **T**ransmission **C**ontrol **P**rotocol (TCP)
  - **U**ser **D**atagram **P**rotocol (UDP)

Speaker notes

In computer networking, a port is an **endpoint of communication** associated with an IP address and protocol type. The most commonly used protocols that use ports are the **T**ransmission **C**ontrol **P**rotocol (TCP) and the **U**ser **D**atagram **P**rotocol (UDP), which are **transport layer** protocols (OSI layer 4).

A port is represented as an unsigned 16-bit number, from 0 to 65,535 (2^{16} - 1).

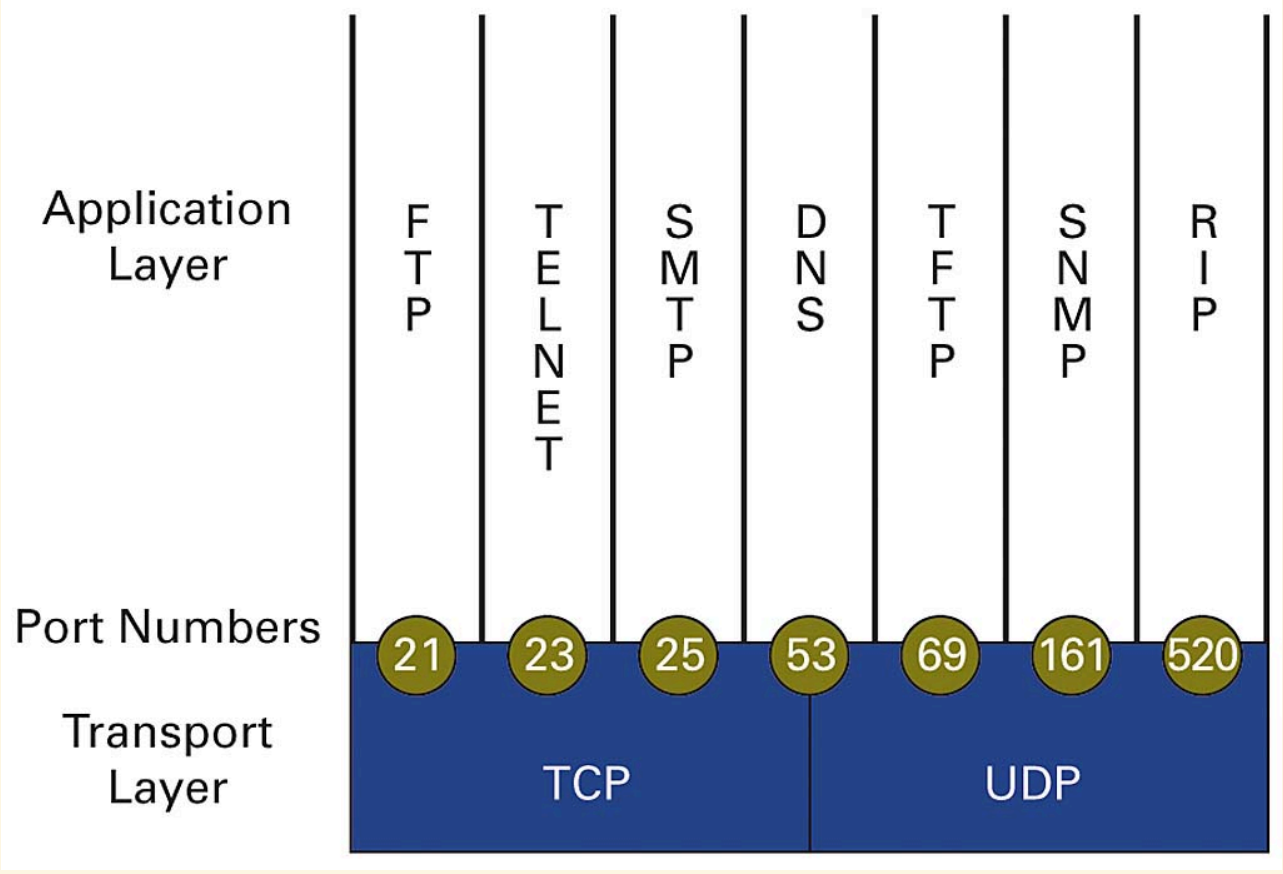
A port number is always associated with an IP address and the type of transport protocol used for communication. For example, when a browser displays a web page, it is making a TCP (or UDP) connection to an IP address on port 80 (HTTP) or 443 (HTTPS).

You can see this information if you access a web page with a command-line HTTP client like cURL:

```
$> curl -v https://google.com
...
** Connected to google.com (142.250.203.110) port 443
...
```

MULTIPLEXING

One IP address, many ports



Speaker notes

A typical computer can be reached at one IP address.

However, one client can **open many connections at the same time to a given IP address and server port** (up to 65535, one for each source port). A client can also open multiple connections to **different ports** at the same time. Ports allow multiplexing at one network address.

For example, a client may open 4 simultaneous TCP connections to a server:

- On port 22 to connect with an SSH client
- On port 25 to retrieve mails with the SMTP protocol
- On port 443 to request a web page with a browser using the HTTPS protocol
- On port 443 (again) to simultaneously retrieve a JavaScript file using the HTTPS protocol

REGISTERED PORT NUMBERS

IANA maintains a list of official of port numbers

Port	Use
22	**S**ecure **Sh**ell (SSH)
80	**H**yper**t**ext **T**ransfer **P**rotocol (HTTP)
443	**H**yper**t**ext **T**ransfer **P**rotocol (**S**ecure) (HTTPS)
5432	PostgreSQL

Speaker notes

The **I**nternet **A**ssigned **N**umbers **A**uthority (IANA) maintains a list of the official assignments of port numbers for specific uses, although this is not always respected in practice.

See the full list.

WELL-KNOWN PORTS

- Ports 0 to 1023
- **Well-known** or **system ports**
- Widely used network services (SSH, HTTP)
- **Superuser privileges** required

Speaker notes

The port numbers in the range from 0 to 1023 are the **well-known ports** or **system ports**. They are used by system processes that provide widely used types of network services, such as SSH or DNS.

On Unix operating systems, a process must execute with **superuser privileges** to be able to bind a network socket on a well-known port.

> *The port numbers in the range from 49152 to 65535 are **dynamic or private ports** that cannot be registered with IANA. This range is used for private or customized services, for temporary purposes, and for automatic allocation of ephemeral ports.*