The future of the Internet

IPv6

IPv4 Address Exhaustion

An IPv4 address is 32 bits long. There's 2^{32} unique addresses, which is around 4,294,967,296 in total.

Depletion is happening due to the growing numbers of :

- Internet users
- Always-On Devices

Countermeasures

- **Network Address Resolution (NAT) protocol** – The modification of IP headers of packets while in transit, so that entire private networks can share one internet-routable IP address.
- **Classless Inter-Domain Routing (CIDR) protocol** – The fine control of how many addresses are allocated to a subnet
- **Internet Protocol version 6 (IPv6) protocol** – The use of 128bit long addresses, providing 2^{128} unique addresses, which is around 340,282,366,920,938,463,463,374,607,431,768,211,456 in total.

Limitations of Countermeasures

NAT– The number of private networks is increasing with the growing number of internet users and always-on devices. Trends such as business digitalisation, or industry 4.0, require each business to have its own private network connected to the internet, so it's likely the number of private networks needed is larger than the total amount of IPv4 addresses.

Classless Inter-Domain Routing (CIDR) protocol – Subnets are likely to require larger numbers of addresses due to Internet of Things (IoT) connectivity demands. According to IoT Analytics (2023) technology such as Low-Power Wide-Area-Networks (LPWAN) and Low Earth Orbit (LEO) satellites are predicted to increase IoT coverage and reliability making IoT devices easier to adopt. Subnets will need to be larger to include them.

Limitations of IPv6

The initial adoption of the protocol requires a bit more effort by developers than sticking to IPv4.

❖IPv6 is not backwards compatible.

❖Not all devices are IPv6 compatible.

❖Migration requires investment.

❖Some Internet Service Providers (ISP) lack IPv6 support.

Motivation for IPv6

The initial adoption of the protocol requires a bit more effort by developers than sticking to IPv4,

BUT using IPv6 will be the only way to continue developing applications that use internet services once all IPv4 addresses are taken. Continuous development will remain essential for a fully digital enterprise (Wei et al., 2019), so the adoption is unavoidable.

IPv6 Security

- **Internet Protocol Security (IPsec) protocol suite** – A suite of protocols for authentication and encryption.
    - **Authentication Header (AH) protocol** – provides data origin authentication, protecting against replay attacks.
    - **Encapsulating Security Payload (ESP) protocol** – provides integrity and confidentiality of data.
    - **Internet Security Association and Key Management (ISAKMP) protocol** - provides a key exchange mechanism necessary for AH and ESP operations
- **Address Scanning Protection**– The time required to scan IPv6 subnet addresses is much longer.
- **Secure Neighbor Discovery (SEND) protocol** – A network discovery protocol with cryptographic verification of node identities

The future of the Internet

DNSSEC

DNS Server Cache Poisoning

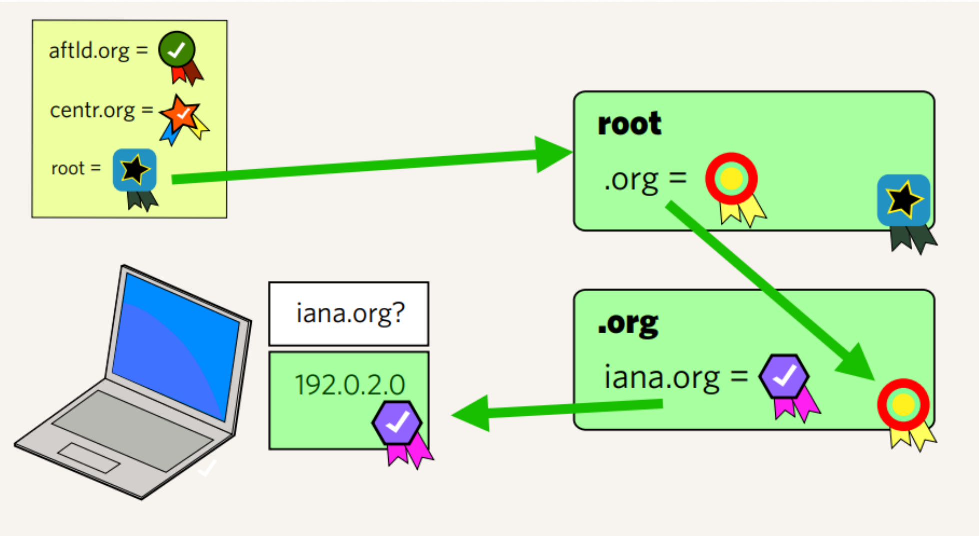
The Domain Name System (DNS) protocol allows for IP addresses to be linked to domain names and vice versa.

A DNS server keeps track of the IP address to domain name pairs, and provides the information upon DNS lookup calls.

A malicious attacker can alter the data stored in a DNS server to provide misleading information; therefore, the DNS protocol is not secure.

Countermeasures

Domain Name System Security Extensions (DNSSEC) protocol – The addition of certificates from a chain of trust to prove information has not been modified.



Limitations of DNSEC

- ❖The deployment of the protocol requires first establishing DNS zone managers to be trusted.
- ❖Significant load is added to DNS servers.
- ❖Political entities are concerned about the centralization.

The future of the Internet

QUIC

Advantages of QUIC

- TLS handshake performed while establishing connection.
- Less time spent waiting compared to TCP
- Encryption