# Infrastructure Security Using Linux

Computer science / Cybersecurity

## Networking and DNS

**13 → 16**

# TCP/IP Networking

# TCP/IP Overview

- ***TCP/IP (Transmission Control Protocol/Internet Protocol)*** is the foundation of Internet networking.
- **Platform-independent**: Works across different hardware and operating systems.
- Enables devices to **interoperate** and exchange data regardless of internal differences.

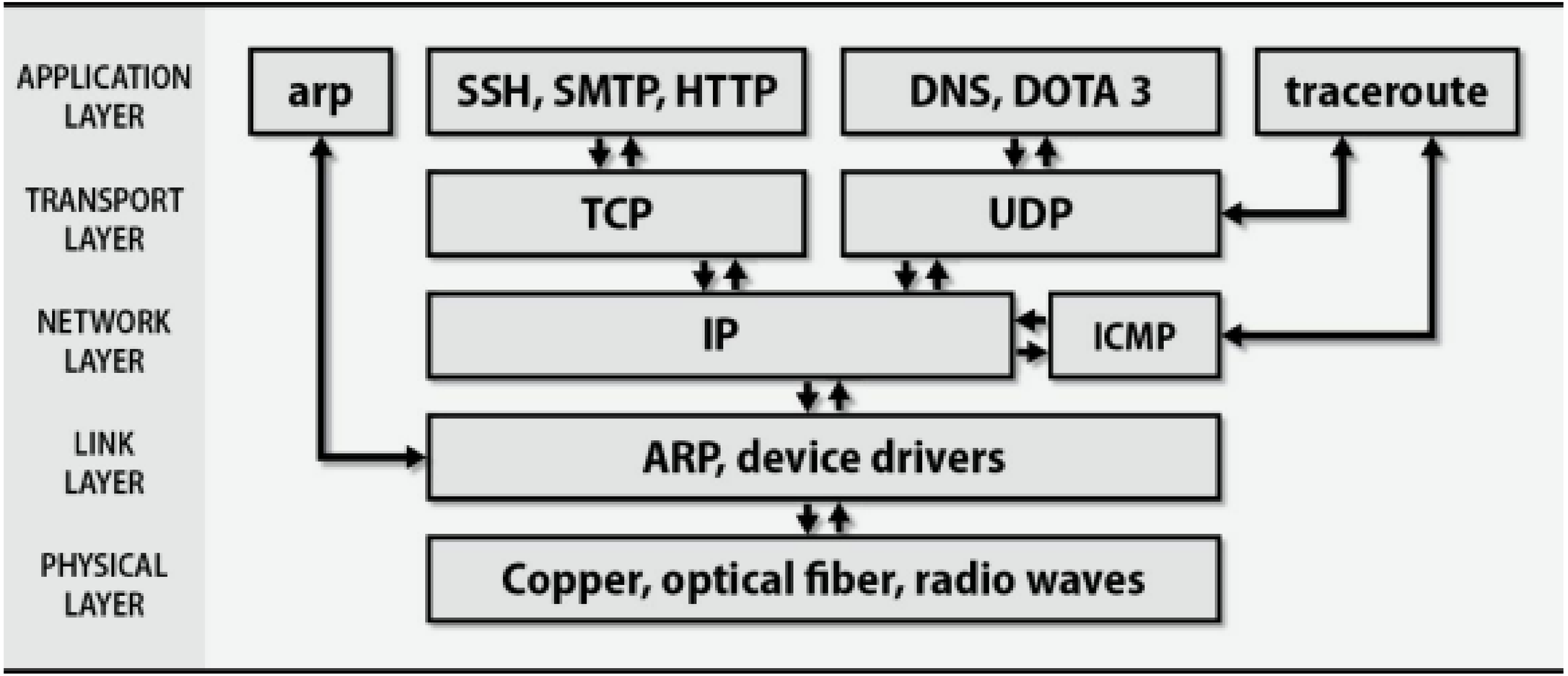
# TCP/IP and the Internet

- Originated from ARPANET, a research network funded by the U.S. Department of Defense (ARPA)
- TCP/IP developed to enable communication across ARPANET
- Modern Internet: a global network of private ISP-owned networks
- ISPs connect through peering points to form the Internet

# Networking Basics

- **IP (Internet Protocol)**: Routes data packets between machines *(RFC 791)*
- **ICMP**: Sends error messages and control info *(RFC 792)*
- **ARP**: Maps IP addresses to MAC addresses *(RFC 826)*
- **UDP**: Sends packets without connection or delivery guarantees *(RFC 768)*
- **TCP**: Sends packets with reliable, ordered delivery *(RFC 793)*

# Exhibit A: TCP/IP layering model



# IPv4 and IPv6

- **IPv4** is the original version of the Internet Protocol. It uses 32-bit addresses, which limits the number of unique addresses to 4,294,967,296.
- **IPv6** is the latest implemented version of the Internet Protocol. It uses 128-bit addresses, which allows for 340,282,366,920,938,463,463,374,607,431,768,211,456 unique addresses.

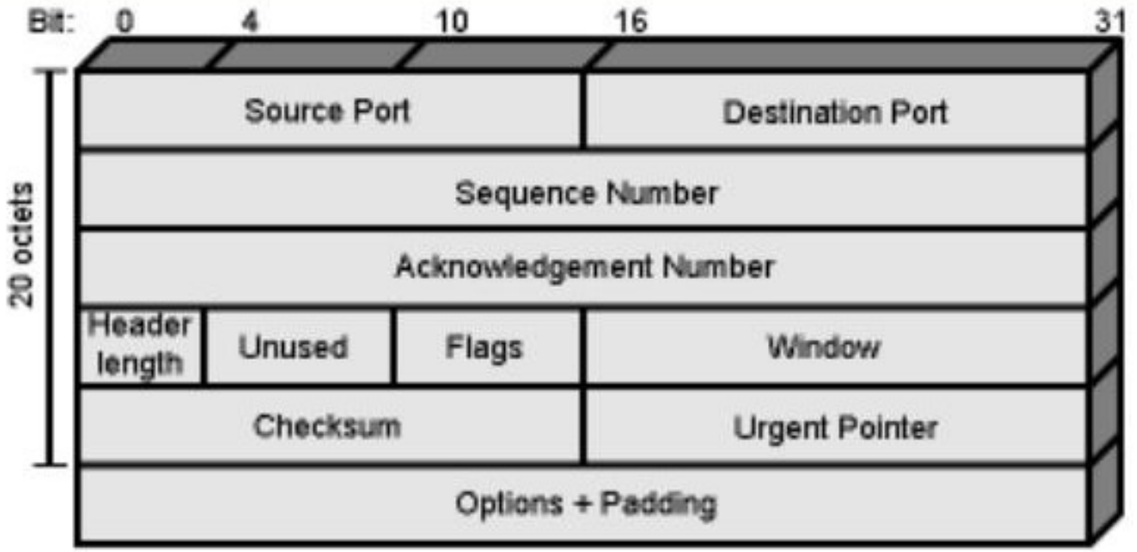
In base 10, $2^{128} =$

$$340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456.$$

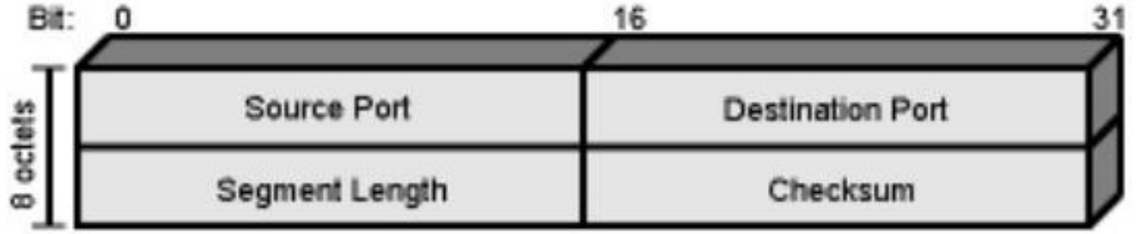
To express it as a power of 10:

$$2^{128} \approx 3.4028 \times 10^{38}$$

# TCP and UDP Headers




(a) TCP Header




(b) UDP Header

# MAC Addressing

- Unique 48-bit identifier for network interfaces
- Used in IEEE 802 networks (e.g., Ethernet, Wi-Fi)
- Format: six pairs of hexadecimal digits (e.g., 00:1A:2B:3C:4D:5E)
- Enables communication on the local network segment

- **Hostname Addressing**
  *IP addresses are numeric and hard to remember*
  **Operating systems map hostnames to IPs using:**
  - *Static file*: etc/hosts
  - *LDAP*
  - *DNS*

# Ports

*A port identifies a specific service or process*

- Allows multiple services to share one IP
- Tied to protocols like *TCP* or *UDP*
- Well-known ports listed in etc/services

- **Address Types**
  - *Unicast*: One-to-one
  - *Broadcast*: One-to-all
  - *Multicast*: One-to-group
  - *Anycast*: One-to-nearest

# Private Addresses and NAT

- *Private addresses* are used within local networks and cannot be routed on the public Internet.
- *NAT (Network Address Translation)* maps private addresses to public ones, enabling communication between private networks and the Internet.

**Private IPv4 Address Range**

| Class | IP Range | CIDR Block |
|---|---|---|
| A | 10.0.0.0 – 10.255.255.255 | 10.0.0.0/8 |
| B | 172.16.0.0 – 172.31.255.255 | 172.16.0.0/12 |
| C | 192.168.0.0 – 192.168.255.255 | 192.168.0.0/16 |

# Security issues

- **IP Forwarding**

  *A system with IP forwarding can function as a router*

  - Receives packets on one interface, forwards them to another
  - Used in systems with multiple network interfaces
  - Should be disabled on non-router systems (use sysctl setting: net.ipv4.ip_forward = 0)

- **ICMP Redirects**

  *ICMP Redirects can be exploited for malicious routing*

  - Attackers can reroute traffic through compromised devices
  - Best practice: disable ICMP redirects (use sysctl setting: net.ipv4.conf.all.accept_redirects = 0)

# Security issues

- **Source Routing**
  *Allows packet senders to define the network path*
  - Can bypass security controls and enable attacks
  - Should be disabled to prevent misuse (sysctl setting: net.ipv4.conf.all.accept_source_route = 0)
- **Smurf Attacks**
  *A denial-of-service attack using ICMP Echo Requests*
  - Amplifies traffic by targeting broadcast addresses
  - Causes all hosts to flood the victim with responses
  - Mitigation: disable ICMP Echo Requests (sysctl setting: net.ipv4.icmp_echo_ignore_all = 1)

# Security issues

- **IP Spoofing**
  *Involves sending packets with forged source IPs to mimic trusted hosts*
  - Used to gain unauthorized access or bypass filters
  - Mitigation: enable IP source address validation (sysctl setting: net.ipv4.conf.all.rp_filter = 1)
  - Use *unicast reverse path forwarding* to drop packets with unreachable source addresses
- **VPN (Virtual Private Network)**
  *A secure, encrypted tunnel between devices*
  - Protects data from snooping and interference
  - Masks IP address and location
  - Uses protocols like *IPsec* or *SSL/TLS* for encryption
  - Routes traffic through a remote server for secure communication

# Hostname and P address assignment

- When you are an admin, you need to maintain a list of IP addresses and hostnames. This list can be maintained in a file, such as **/etc/hosts**, or in a DNS server.

```
127.0.0.1          localhost
::1                localhost ip6-localhost
ff02::1            ip6-allnodes
ff02::2            ip6-allrouters
192.108.21.48      lollipop.atrust.com lollipop loghost
192.108.21.254     chimchim-gw.atrust.com chimchim-gw
192.108.21.1       ns.atrust.com ns
192.225.33.5       licenses.atrust.com license-server
```

# Physical Networking (Ethernet)

- *The dominant LAN technology, used globally in various forms*
  - Originated from Bob Metcalfe's Ph.D. thesis, now defined by IEEE standards
  - Most common physical networking method
  - Uses twisted-pair cables with RJ-45 connectors
  - Deployed in both *LANs* and *WANs*

**Table 14.1: The evolution of Ethernet**

| Year | Speed | Common name | IEEE# | Dist | Media[a] |
|---|---|---|---|---|---|
| 1973 | 3 Mb/s | Xerox Ethernet | – | ? | Coax |
| 1976 | 10 Mb/s | Ethernet 1 | – | 500m | RG-11 coax |
| 1989 | 10 Mb/s | 10BASE-T | 802.3 | 100m | Cat 3 UTP copper |
| 1994 | 100 Mb/s | 100BASE-TX | 802.3u | 100m | Cat 5 UTP copper |
| 1999 | 1 Gb/s | 1000BASE-T ("gigabit") | 802.3ab | 100m | Cat 5e, 6 UTP copper |
| 2006 | 10 Gb/s | 10GBASE-T ("10 gig") | 802.3an | 100m | Cat 6a, 7, 7a UTP |
| 2009 | 40 Gb/s | 40GBASE-CR4 | P802.3ba | 10m | UTP copper |
| | | 40GBASE-SR4 | | 100m | MM fiber |
| 2009 | 100 Gb/s | 100GBASE-CR10 | P802.3ba | 10m | UTP copper |
| | | 100GBASE-SR10 | | 100m | MM fiber |
| 2018[b] | 200 Gb/s | 200GBASE-FR4 | 802.3bs[c] | 2km | CWDM fiber |
| | | 200GBASE-LR4 | | 10km | CWDM fiber |
| 2018[b] | 400 Gb/s | 400GBASE-SR16 | 802.3bs | 100m | MM fiber (16 strand) |
| | | 400GBASE-DR4 | | 500m | MM fiber (4 strand) |
| | | 400GBASE-FR8 | | 2km | CWDM fiber |
| | | 400GBASE-LR8 | | 10km | CWDM fiber |
| 2020[b] | 1 Tb/s | TbE | TBD | TBD | TBD |

a. MM = Multimode, SM = Single-mode, UTP = Unshielded twisted pair, CWDM = Coarse wavelength division multiplexing

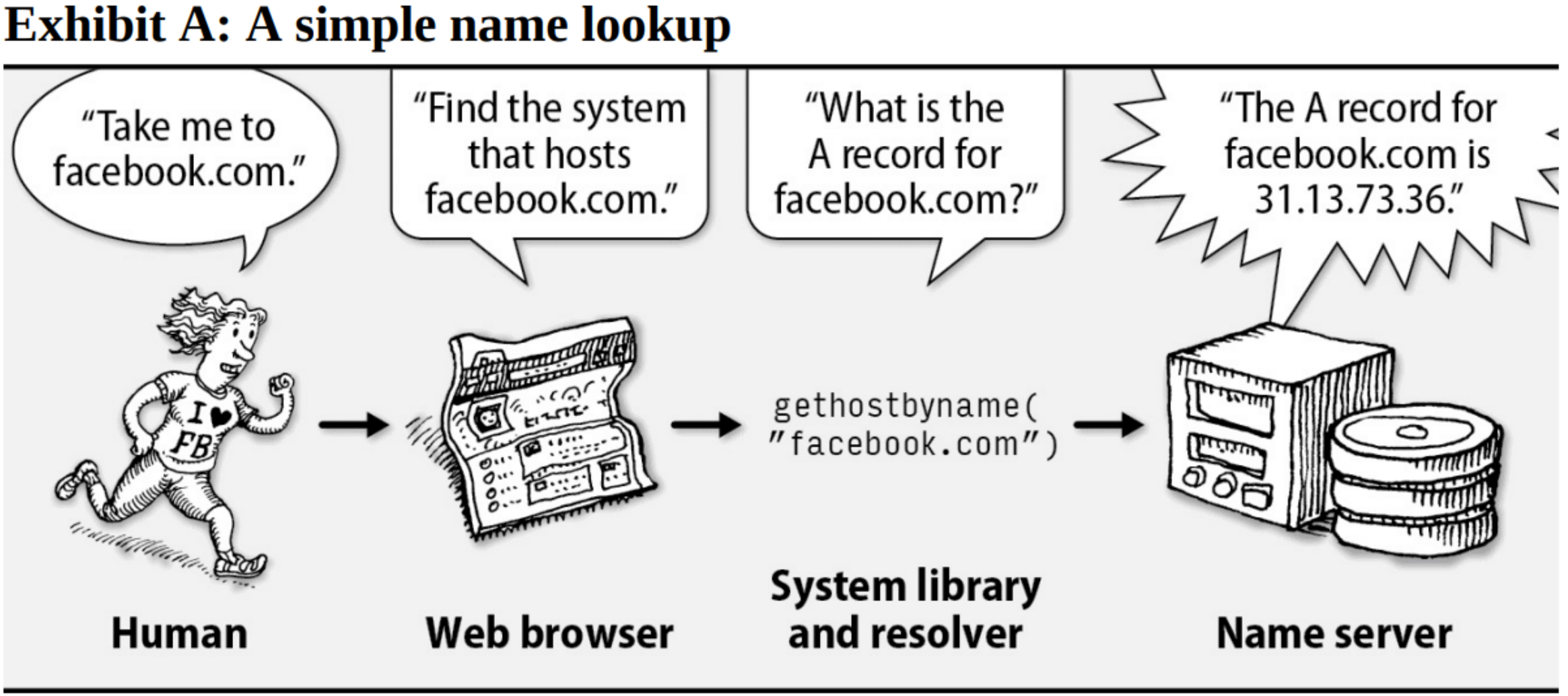
b. Industry projection

c. We'll give the benefit of the doubt and assume this lettering choice was an unfortunate coincidence.

# DNS

The Domain Name System

# Queries and Responses



# DNS for looks (Resolver)

*Each host should act as a DNS client*

- Configuration is done
  - ***NS ns1.atrust.com.***
  - ***NS ns2.atrust.com.***
  - ***NS ns3.atrust.com.***

| | Type | Name | Function |
|---|---|---|---|
| Zone | SOA | Start Of Authority | Defines a DNS zone |
| | NS | Name Server | Identifies servers, delegates subdomains |
| Basics | A | IPv4 Address | Name-to-address translation |
| | AAAA | IPv6 Address | Name-to-IPv6-address translation |
| | PTR | Pointer | Address-to-name translation |
| | MX | Mail Exchanger | Controls email routing |
| Security | DS | Delegation Signer | Hash of signed child zone's key-signing key |
| | DNSKEY | Public Key | Public key for a DNS name |
| | NSEC | Next Secure | Used with DNSSEC for negative answers |
| | NSEC3 | Next Secure v3 | Used with DNSSEC for negative answers |
| | RRSIG | Signature | Signed, authenticated resource record set |
| Optional | CNAME | Canonical Name | Nicknames or aliases for a host |
| | SRV | Service | Gives locations of a well-known service |
| | TXT | Text | Comments or untyped information |