IT/CYBR 4323, Chapter 10:

IPv4 Companion Protocols

- Mr. Donald Privitera, with Mr. Gennadiy Kemelmakher
- Kennesaw State University
- Marietta Campus
- College of Computing and Software Engineering
- IT Department
- dprivit2@kennesaw.edu

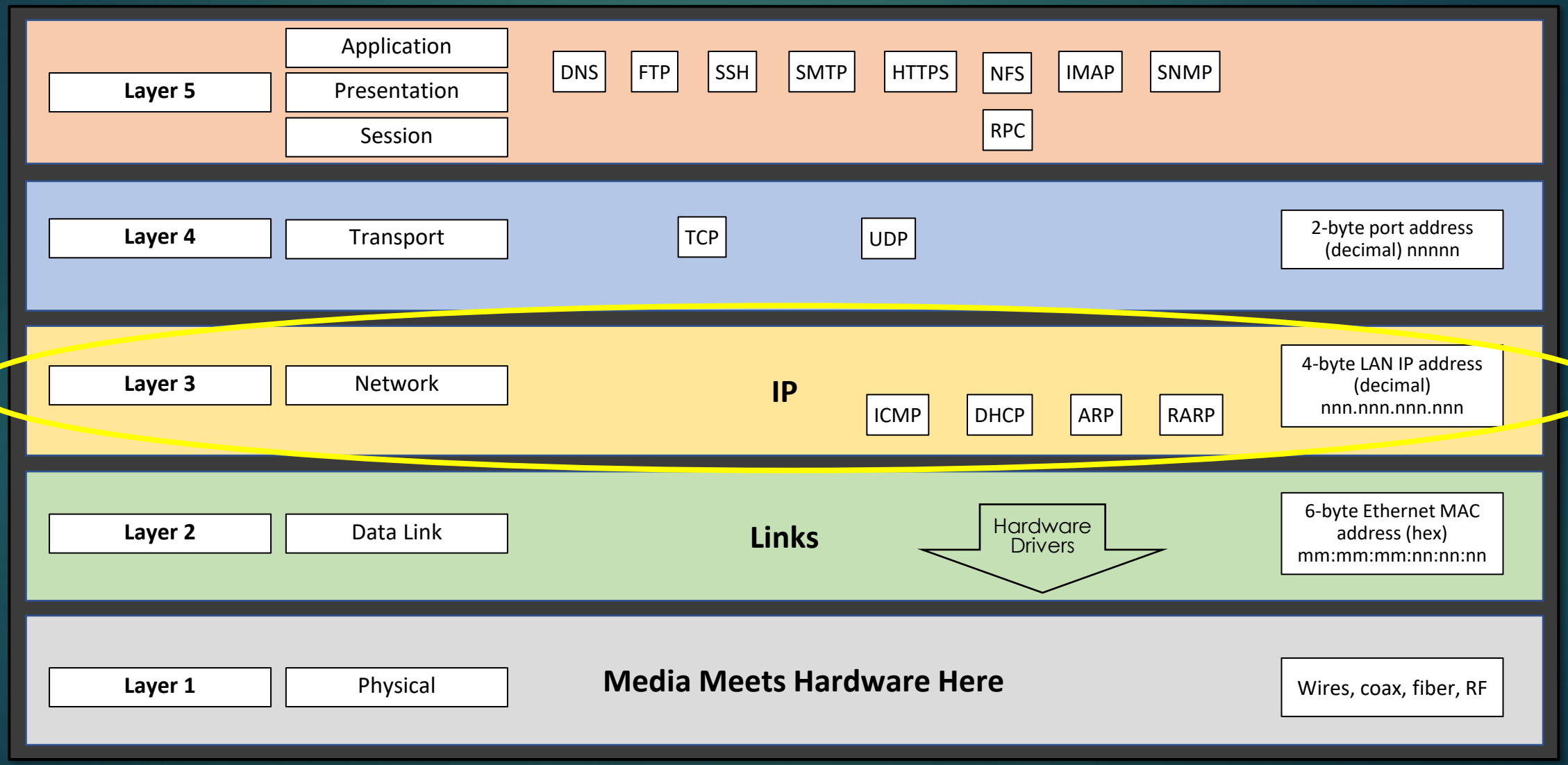
Content:

We are going to cover companion protocols that make IP easier to work with. These protocols are considered to co-exist at layer 3 along with IP.

1. DNS: Domain Name System
2. ARP: Address Resolution Protocol (absolutely required)
3. DHCP: Dynamic Host Configuration Protocol
4. ICMP: Internet Control Message Protocol

Upon completing this module, you should be able to setup, use, and troubleshoot issues with these companion protocols.

TCP/IP 5-Layer Network Stack



DNS

- Domain Name System translates human-readable host names, such as intronetworks.cs.luc.edu to IP addresses.
- DNS is distributed over thousands of DNS servers. Each domain is responsible for maintaining its own DNS servers to translate names to addresses. All DNS servers share information over time. This is known as propagation.
- Local routers can act as a DNS server.
- There are authoritative (your local DNS server resolves without asking another server) and non-authoritative name servers.
- DNS Zone is a specific portion of the DNS namespace in the Domain Name System (DNS), which is managed by a specific organization or administrator.

Domain Names

- Top-level domains are assigned by ICANN https://www.icann.org/
- The original top-level domains were seven three-letter domains – .com, .net, .org, .int, .edu, .mil and .gov – and the two-letter country-code domains (eg .us for USA, .Ca for Canada, etc.).
- Now there are hundreds of non-country top-level domains, such as .aero, .biz, .info, etc.
- Domain names (and subdomain names) can also contain unicode characters, so as to support national alphabets.

Major DNS Record Types

- A = Address records for IPv4 addresses.
- AAAA = Address records for IPv6 addresses.
- CAA = Certification Authority Authorization acceptable CAs for a host/domain.
- CNAME = Canonical Name is a synonym for another name.
- DNSKEY = Key record used in DNS Security (DNSSEC).
- DS = Delegation Signer used to identify the DNSSEC signing key of a zone.
- MX = The address of a Mail Exchange within the Internet email system, a **message transfer agent** (**MTA**), or **mail transfer agent**, or **mail relay** is software that transfers electronic mail messages from one computer to another using SMTP.
- NS = Name Server delegates a DNS Zone to use the given authoritative name server.
- SOA = Start of Authority specified authoritative info about a DNS zone.
- SRV = Service location record for general info
- TXT = Originally for human readable text; now for data DKIM, DMARC, etc.
- https://en.wikipedia.org/wiki/List_of_DNS_record_types

Domain Name Resolution

- DNS is resolved in a hierarchical manner.
- **intronetworks.cs.luc.edu** is resolved as follows:
- **edu**: the top-level domain (TLD) for educational institutions in the US
- **luc**: Loyola University Chicago
- **cs**: The Loyola Computer Science Department
- **intronetworks**: a hostname associated to a specific IP address
- (domain names luc.edu and cs.luc.edu happen to be valid hostnames as well)

DIG

- DIG = Domain Information Groper
- This utility is used to show DNS records and other domain information.
- DIG is more useful and complete than NSLOOKUP which was deprecated on Linux.
- Below is a link to an online DIG utility:
- https://toolbox.googleapps.com/apps/dig/

Top Level Domains (TLDs)

- ICANN still must approve all new top-level domains. Applications are accepted only during specific intervals; the application fee is US$3,500, for TLD it is US$185,000 (per icann.org).

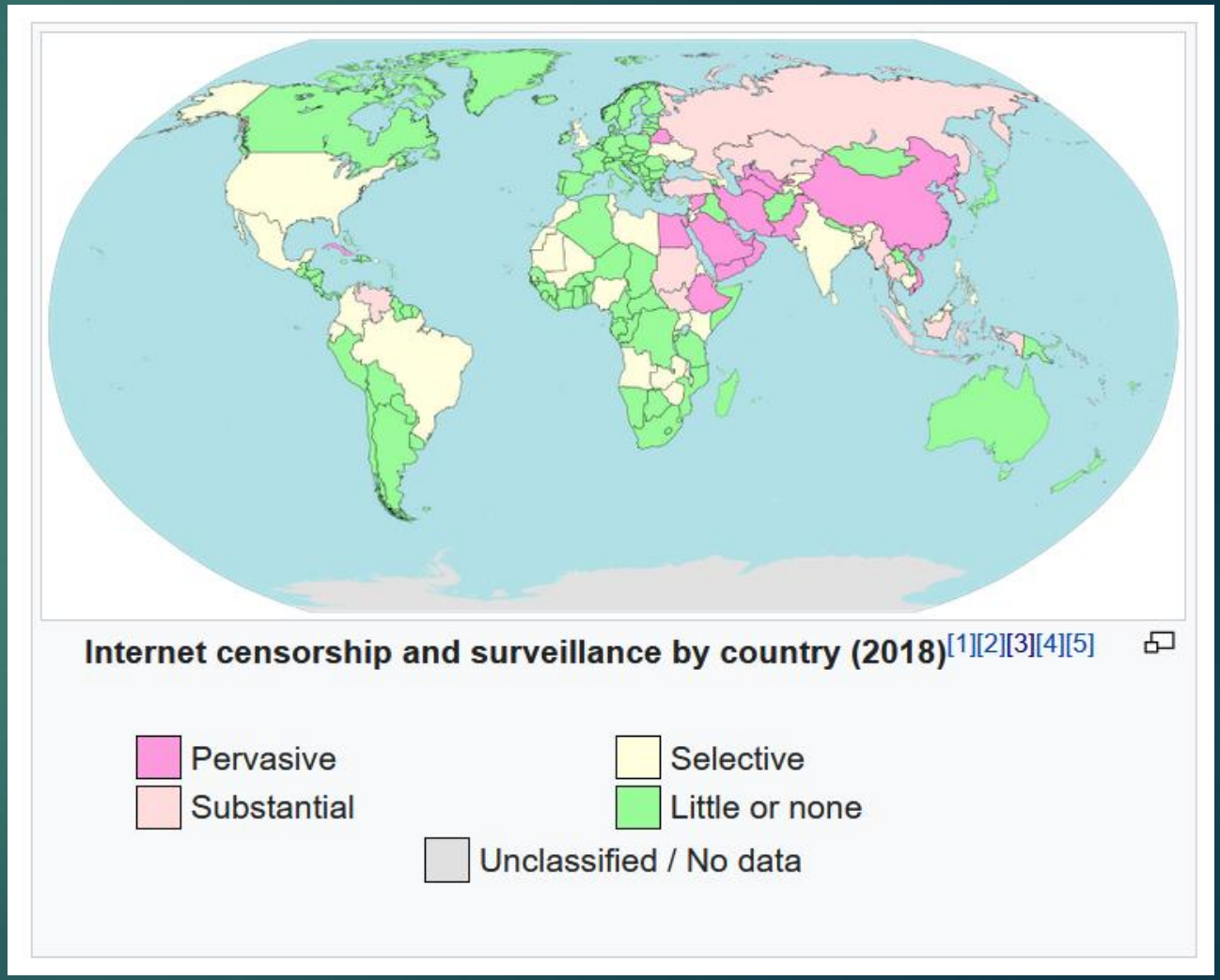
- The actual leasing of domain names to companies and individuals is done by organizations known as domain registrars who work under contract with ICANN.

DNS Filtering

- DNS can be used as a filtering layer for security and policy compliance.
- For example, Cisco OpenDNS (https://www.opendns.com/) provides these capabilities.
- Addresses are checked in real-time against a variety of factors.
- Web traffic can be analyzed to determine if it is safe and meets company policy.
- All of this is done at the DNS side and does not impact user systems.
- An extreme version of this can be used for censorship (Russia, China, North Vietnam, etcetera). https://en.wikipedia.org/wiki/Internet_censorship

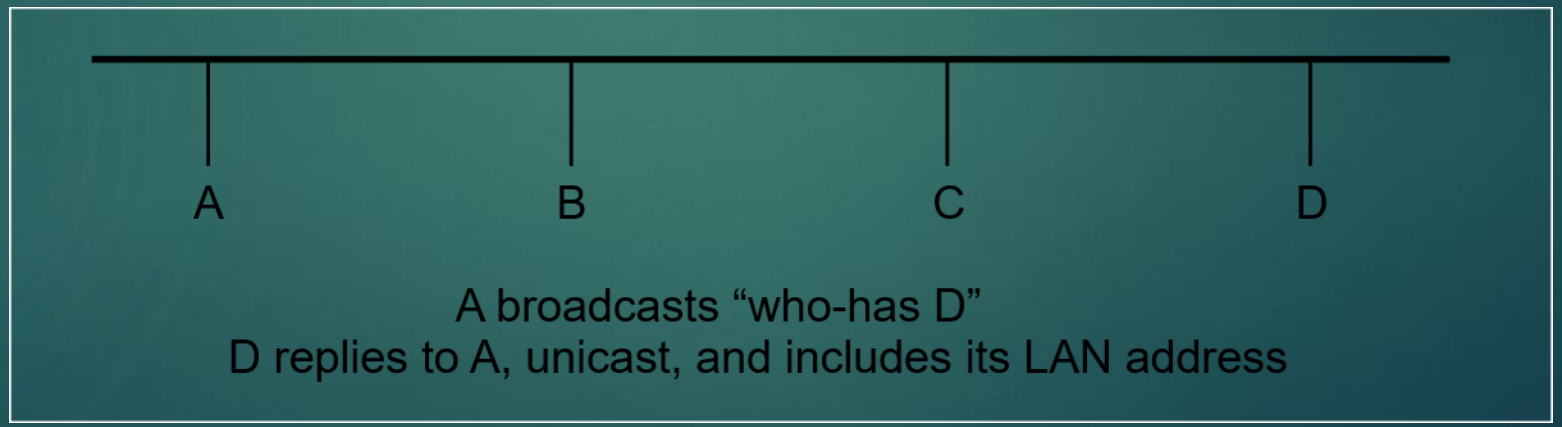
Internet Censorship

- DNS filtering may be used for censorship purposes
- https://en.wikipedia.org/wiki/Internet_censorship_and_surveillance_by_country#cite_note-RWBEnemies2014-3



Address Resolution Protocol (ARP)

- host A sends out a broadcast ARP query or "who-has DIP?" request, which includes A's own IPv4 and LAN addresses. All hosts on the LAN receive this message. The host for whom the message is intended, D, will recognize that it should reply, and will return an ARP reply or "is-at" message containing DLAN. Because the original request contained ALAN, D's response can be sent directly to A, that is, unicast.



ARP Concepts

- self-ARP, or gratuitous ARP = Most hosts today implement self-ARP, or gratuitous ARP, on startup (or wakeup): when station A starts up it sends out an ARP query for itself: "who-has A?". Two things are gained from this: first, all stations that had A in their cache are now updated with A's most current ALAN address, in case there was a change, and second, if an answer is received, then presumably some other host on the network has the same IPv4 address as A (basic duplicate address detection).
- Address Conflict Detection (ACD) = A host using ACD sends out three ARP queries for its new IPv4 address, spaced over a few seconds and leaving the ARP field for the sender's IPv4 address filled with zeroes. This last step means that any other host with that IPv4 address in its cache will ignore the packet, rather than update its cache. If the original host receives no replies, it then sends out two more ARP queries for its new address, this time with the ARP field for the sender's IPv4 address filled in with the new address; this is the stage at which other hosts on the network will make any necessary cache updates. Finally, ACD requires that hosts that do detect a duplicate address must discontinue using it.

ARP Spoofing

- ARP Spoofing = Suppose A wants to log in to secure server S, using a password. How can B (for Bad) impersonate S?
- Here is an ARP-based strategy, sometimes known as ARP Spoofing. First, B makes sure the real S is down, either by waiting until scheduled downtime or by launching a denial-of-service attack against S.
- When A tries to connect, it will begin with an ARP "who-has S?". All B has to do is answer, "S is-at B". There is a trivial way to do this: B simply needs to set its own IP address to that of S.
- A will connect, and may be convinced to give its password to B. B now simply responds with something plausible like "backup in progress; try later", and meanwhile use A's credentials against the real S.
- Only public key encryption with digital certificates for authentication can mitigate this man-in-the-middle risk.

ARP failover and sniffer detection

- ARP Failover = ARP can be setup for resiliency to have a backup ARP server in case the primary ARP server fails.
- Detecting sniffers = ARP messages can be used to send an ARP request to a non-existent address which cause any host in promiscuous mode to repeat the message and give itself away.

ARP Multihomed hosts

- Multihomed hosts = If host A has two interfaces iface1 and iface2 on the same LAN, with respective IP addresses A1 and A2, then it is common for the two to be used interchangeably. Traffic addressed to A1 may be received via iface2 and vice-versa, and traffic from A1 may be sent via iface2. In 9.2.1 Multihomed hosts this is described as the weak end-system model; the idea is that we should think of the IP addresses A1 and A2 as bound to A rather than to their respective interfaces.
- In support of this model, ARP can usually be configured (in fact this is often the default) so that ARP requests for either IP address and received by either interface may be answered with either physical address. Usually all requests are answered with the physical address of the preferred (ie faster) interface.

Dynamic Host Control Protocol (DHCP)

- Very important for managing dynamic network addressing in IPv4.
- Started out as Reverse ARP (RARP) then evolved into BOOTP and then to its present form.
- DHCP involves a host, at startup, broadcasting a query containing its own LAN MAC address, and having a server reply telling the host what IPv4 address is assigned to it, hence the "Reverse ARP" name.
- The DHCP response message is also likely to carry, piggybacked onto it, several other essential startup options. Unlike the IPv4 address, these additional network parameters usually do not depend on the specific host that has sent the DHCP query; they are likely constant for the subnet or even the site. In all, a typical DHCP message includes the following:
  - IPv4 address
  - subnet mask
  - default router
  - DNS Server
- These four items are a standard minimal network configuration; in practical terms, hosts cannot function properly without them. Most DHCP implementations support the piggybacking of the latter three above, and a wide variety of other configuration values, onto the server responses.

Internet Control Message Protocol (ICMP)

Type	***Description***
Echo Request	ping queries
Echo Reply	ping responses
Destination Unreachable	Destination **network** unreachable
	Destination **host** unreachable
	Destination **port** unreachable
	Fragmentation required but DF flag set
	Network administratively prohibited
Source Quench	Congestion control
Redirect Message	Redirect datagram for the **network**
	Redirect datagram for the **host**
	Redirect for TOS and network
	Redirect for TOS and host
Router Solicitation	Router discovery/selection/solicitation
Time Exceeded	TTL expired in transit
	Fragment reassembly time exceeded
Bad IP Header or Parameter	Pointer indicates the error
	Missing a required option
	Bad length
Timestamp Timestamp Reply	Like ping, but requesting a timestamp from the destination

Peter L Dordal, An Introduction to Computer Networks

Internet Control Message Protocol (ICMP) [slide 1 of 3]

- ICMP best known as protocol that enables Ping (echo request/reply)
- The Echo and Timestamp formats are queries, sent by one host to another. Most of the others are all error messages, sent by a router to the sender of an offending packet. Redirect and Router Solicitation messages are informational but follow the error-message format. Query formats contain a 16-bit Query Identifier, assigned by the query sender and echoed back by the query responder.
- Source Quench is no longer used.

Internet Control Message Protocol (ICMP) [slide 2 of 3]

- Destination Unreachable type has a large number of subtypes:
- Network unreachable: some router had no entry for forwarding the packet, and no default route
- Host unreachable: the packet reached a router that was on the same LAN as the host, but the host failed to respond to ARP queries
- Port unreachable: the packet was sent to a UDP port on a given host, but that port was not open. TCP, on the other hand, deals with this situation by replying to the connecting endpoint with a reset packet. Unfortunately, the UDP Port Unreachable message is sent to the host, not to the application on that host that sent the undeliverable packet, and so is close to useless as a practical way for applications to be informed when packets cannot be delivered.
- Fragmentation required but DF flag set: a packet arrived at a router and was too big to be forwarded without fragmentation. However, the Don't Fragment bit in the IPv4 header was set, forbidding fragmentation.
- Administratively Prohibited: this is sent by a router that knows it can reach the network in question, but has configureintro to drop the packet and send back Administratively Prohibited messages. A router can also be configured to blackhole messages: to drop the packet and send back nothing.

Internet Control Message Protocol (ICMP) [slide 3 of 3]

- Traceroute uses ICMP messages with TTL incremented by 1 for each successive router discovered by an ICMP Time Exceeded message.
- Routers use ICMP redirect and solicitation messages as an integral part of sending messages to learn about routes to other routers on the network.

References

- An Introduction to Computer Networks — An Introduction to Computer Networks, desktop edition 2.0.6 (luc.edu)
- https://en.wikipedia.org/wiki/List_of_DNS_record_types
- https://toolbox.googleapps.com/apps/dig/
- https://www.opendns.com
- https://en.wikipedia.org/wiki/Internet_censorship
- https://en.wikipedia.org/wiki/Internet_censorship_and_surveillance_by_country#cite_note-RWBEnemies2014-3