TTM4175 Introduction to Communication Technology and data security

Technical information gathering

NTNU
Norwegian University of Science and Technology

Laszlo Erdödi
laszlo.erdodi@ntnu.no

Lecture Overview

- What are the technical information of the target
- How to collect the technical information
- Typical network layouts
- Identifying the network range of the target

Technical information

- Domain names of the target
- Domain owner(s) of the target
- Domain registrants
- Ip addresses associated with the target websites
- Ip ranges of the target
- Ip range owner(s)
- List of hosted websites
- Hosting companies
- Etc

Domain names

A **domain name** is an identification string that defines a realm of administrative autonomy, authority or control within the Internet.

Example: **aftenposten.no**

second level domain.topleveldomain

Domain names are formed by the rules and procedures of the Domain Name System (DNS). Any name registered in the DNS is a domain name.

Top level domain can be (com, net, info, edu, org and country code) Second and third level domains can be any string. The full length of the domain cannot be longer than 255 characters.

innsida.ntnu.no

Domain names

collections.vm.ntnu.no

hostname.thirdlevel.secondlevel.TLD

- A hostname is a domain name that has at least one associated IP address
- The first domain was registered in 1985 (symbolics.com)
- Domains are registered by the domain registrars that are accredited by the Internet Corporation for Assigned Names and Numbers (ICANN)
- each TLD is maintained and serviced technically by an administrative organization operating a registry (*UNINETT Norid AS* for .no)
- All data has to be published and accessible with the *whois* protocol

Domain name registration data – whois (e.g. http://who.is)

The *whois* database must contain the following information:

- Administrative contact
- Technical contact
- Billing contact
- Name servers

Nameservers are computers that provide subdomain information for the particular domain using the *dns* protocol

```
Registrant Contact Information:
        Name                    Domain Name Manager
        Organization            Turner Broadcasting System, Inc.
        Address                 One CNN Center
        City                    Atlanta
        State / Province        GA
        Postal Code             30303
        Country                 US
        Phone                   +1.4048275000
        Fax                     +1.4048271995
        Email                   tngroup@turner.com

Administrative Contact Information:
        Name                    Domain Name Manager
        Organization            Turner Broadcasting System, Inc.
        Address                 One CNN Center
        City                    Atlanta
        State / Province        GA
        Postal Code             30303
        Country                 US
        Phone                   +1.4048275000
        Fax                     +1.4048271995
        Email                   tngroup@turner.com

Technical Contact Information:
        Name                    Domain Name Manager
        Organization            Turner Broadcasting System, Inc.
        Address                 One CNN Center
        City                    Atlanta
        State / Province        GA
        Postal Code             30303
        Country                 US
        Phone                   +1.4048275000
        Fax                     +1.4048271995
        Email                   tngroup@turner.com
```

Domain names

- Unique name with country code (TLD)
- Domain names belong to private individuals or companies
- Everyone can register a domain (for trademarks there's a priority)
- A domain name is only the right to use a special string, it is not an ip and not a computer!

Who holds the domain name?

ntnu.no | SEARCH

Copy result link

Domain name
ntnu.no

Registered: 14-11-1999
Last updated: 15-11-2020

Holder
NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET NTNU

Organization number 974767880

Høgskoleringen 1
NO-7491 Trondheim
Norway

Jan.Kaaro@ntnu.no
+47 73 59 50 00

Incorrect or outdated information? Contact your registrar to correct.

Registrar
UNINETT AS

Abels gate 5
7465 TRONDHEIM
NO-7030 Trondheim
Norway

kontakt@uninett.no
http://www.uninett.no
+47 73 55 79 00

Domain name owner examples

Find the owner of the following domains:

- nrk.no
- dyreparken.no
- horsepro.no

Find a contact phone number for the following domains:

- footish.se
- termesangiovanni.it

When is the expiration date of the following domains:

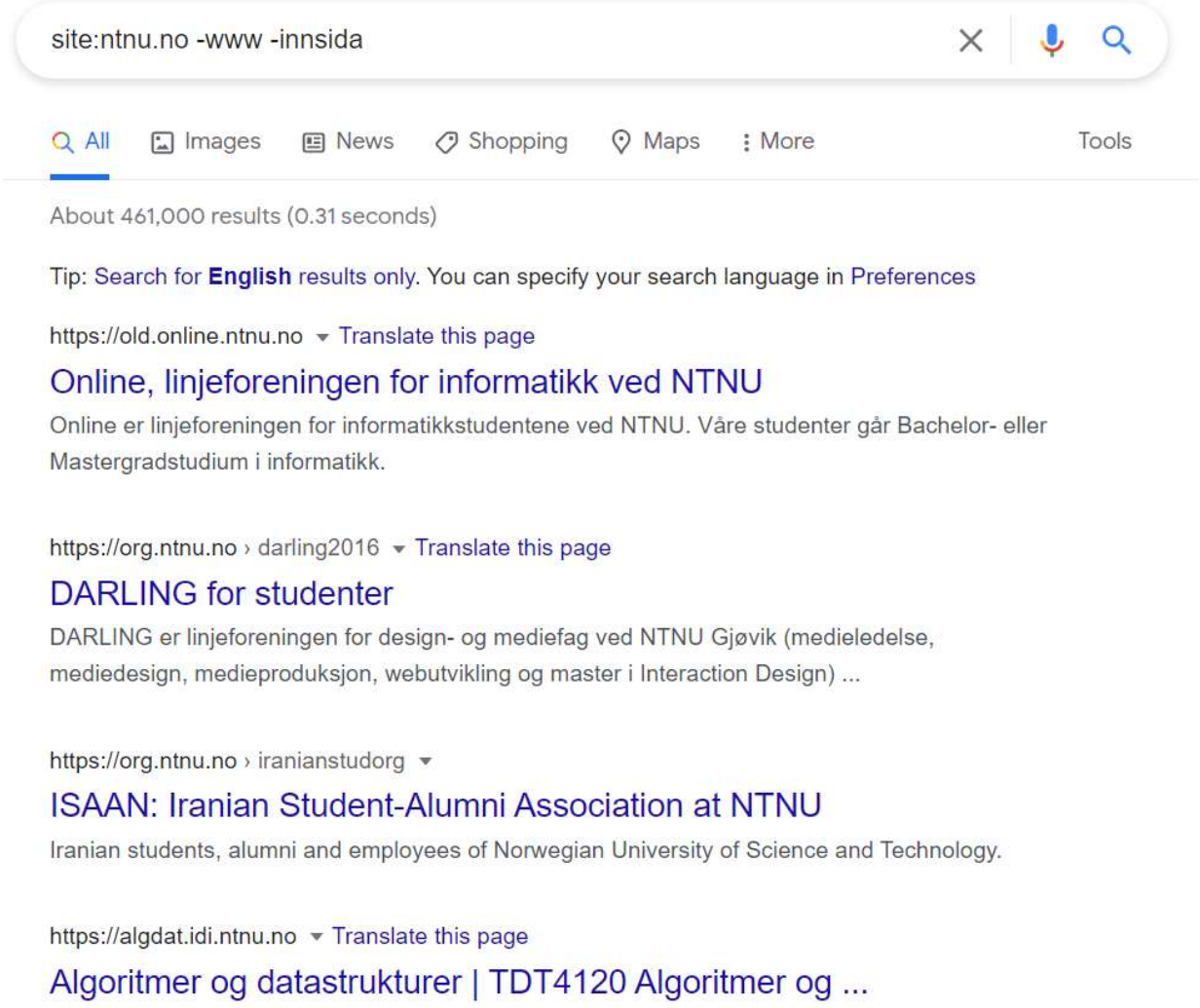
- timeanddate.com

Domain name search

- Example1: find third level domains for *ntnu.no*!

Use the Google with the site: keyword

- Example2: find third level domains for dn.no!



Domain name search - Netcraft

- Finding domains with its owner
- OS version detection

Services ▾ Solutions ▾ News Company ▾ Resources ▾ Report Fraud Request Trial

77 results (showing 1 to 20)

Rank	Site	First seen	Netblock	OS	Site Report
1	**ntnu**.blackboard.com	March 2017	A100 ROW GmbH	Linux	
2	www.math.**ntnu**.no	Febuary 1998	Norwegian University of Science and Technology	Linux - Ubuntu	
3	wiki.math.**ntnu**.no	October 2012	Norwegian University of Science and Technology	Linux - Ubuntu	
4	www.**ntnu**.edu	August 2010	Norwegian University of Science and Technology	Linux - Ubuntu	
5	www.**ntnu**.no	August 2006	Norwegian University of Science and Technology	Linux - Ubuntu	
6	innsida.**ntnu**.no	July 2000	Norwegian University of Science and Technology	Linux - Ubuntu	
7	**ntnu**.cloud.panopto.eu	July 2020	Amazon Data Services Ireland Limited	Linux	
8	**ntnu**.inspera.no	Febuary 2018	Amazon Data Services Ireland Limited	Linux	
9	tma4105.math.**ntnu**.no	June 2019	Norwegian University of Science and Technology	Linux - Ubuntu	
10	stack.math.**ntnu**.no	January 2020	Norwegian University of Science and Technology	Linux - Ubuntu	

Domain name search – Pentest tools

ns1.ntnu.no	129.241.0.208					
ns2.ntnu.no	129.241.0.209					
ftp.ntnu.no	129.241.30.64		Apache 2.4.41			Index of /
nav.ntnu.no	129.241.34.77		Apache			403 Forbidden
mail.ntnu.no	129.241.34.139	Windows	Microsoft-IIS 10.0	ASP.NET 4.0.30319		Outlook
autodiscover.ntnu.no	129.241.34.139	Windows	Microsoft-IIS 10.0	ASP.NET 4.0.30319		Outlook
apps.ntnu.no	129.241.38.20		Apache	PHP 7.1.33		NTNU Apps - Login
mx.ntnu.no	129.241.56.67					
stud.ntnu.no	129.241.56.200		Apache 2.4.29	JSP		NTNU Alumni – Nettverk for tidligere studenter - NTNU
data.ntnu.no	129.241.56.200		Apache 2.4.41			Adresse for publisering av Ã¥pne data
webmail.ntnu.no	129.241.56.200		Apache 2.4.41			NTNU webmail
projects.ntnu.no	129.241.59.100					
vpn1.ntnu.no	129.241.78.10					
vpn.ntnu.no	129.241.78.14					
vpn2.ntnu.no	129.241.78.14					

IP addresses

- IPv4: 32bit (2^{32}=4 294 967 296 combinations)
- IPv6: 128bit (2^{128}=3.4*10^{38} combinations)

- IP addresses are for the identification of computers during the communication (OSI 3rd layer, see later).
- In order to be easy to memorize it, 8bit (byte) blocks are used for ipv4 e.g. **129.240.171.52**
- For ipv6 addresses are represented as eight groups of four hexadecimal digits e.g. **2001:0db8:0000:0042:0000:8a2e:0370:7334**

IP ranges – classful networking

IP ranges contain more ip addresses. e.g. 129.240.171.56—129.240.171.63 (8 addresses)

In 1981 the **classfull networking** was created. It consisted of the A, B, and C class of network ranges.

The idea was to divide the ip into the network and subnet part: **129.240.** **171.58**

identifies the network identifies the host within the network

Class A: 0.0.0.0	-127.255.255.255	128 ranges 2563 in 1 range
Class B: 128.0.0.0	- 191.255.255.255	16384 ranges 2562 in 1 range
Class C: 192.0.0.0	– 223.255.255.255	2097152 ranges 256 in 1 range

IP Ranges: Classless InterDomain Routing (CIDR)

- CIDR was created in 1993
- Network address length is arbitrary (not only 8,16,24 bits)

Examples:

129.240.171.56 (**10000001.11110000.10101011.00111**000) –
129.240.171.63 (**10000001.11110000.10101011.00111**111)

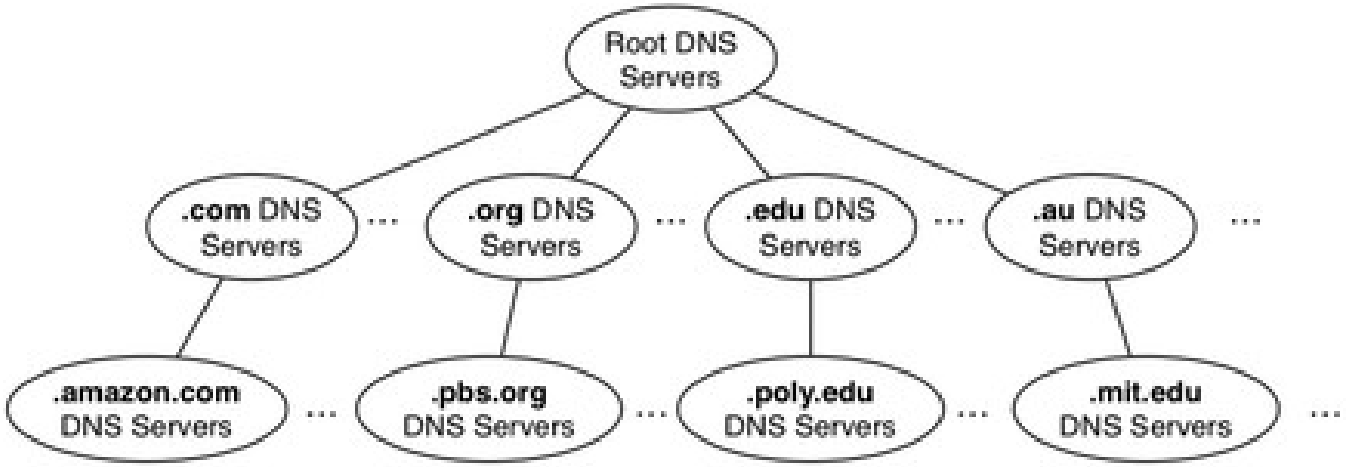
The first 29 bits are fixed in the range, the last three can be anything within the network: **CIDR: 129.240.171.56/29**

130.18.0.0 (**10000010.00010010**.00000000.00000000) –
130.19.255.255 (**10000010.00010011**.11111111.11111111)
130.18.0.0/15

IP Ranges CIDR - examples

- What is the first and last address of the /23 network range that contains: 194.172.10.10?
- What is the first and last address of the /18 network range that contains: 164.44.20.52?
- How many addresses does a /25 network range have?

Domain to ip conversion (DNS service)



- DNS servers are all around the world
- Organized in tree structure (13 root servers)
- The top level domains (.com, .net, .edu, .no, .de, etc.) are directly under the root servers
- DNS data are stored redundantly (master and slave server)

Domain to ip conversion (DNS service)

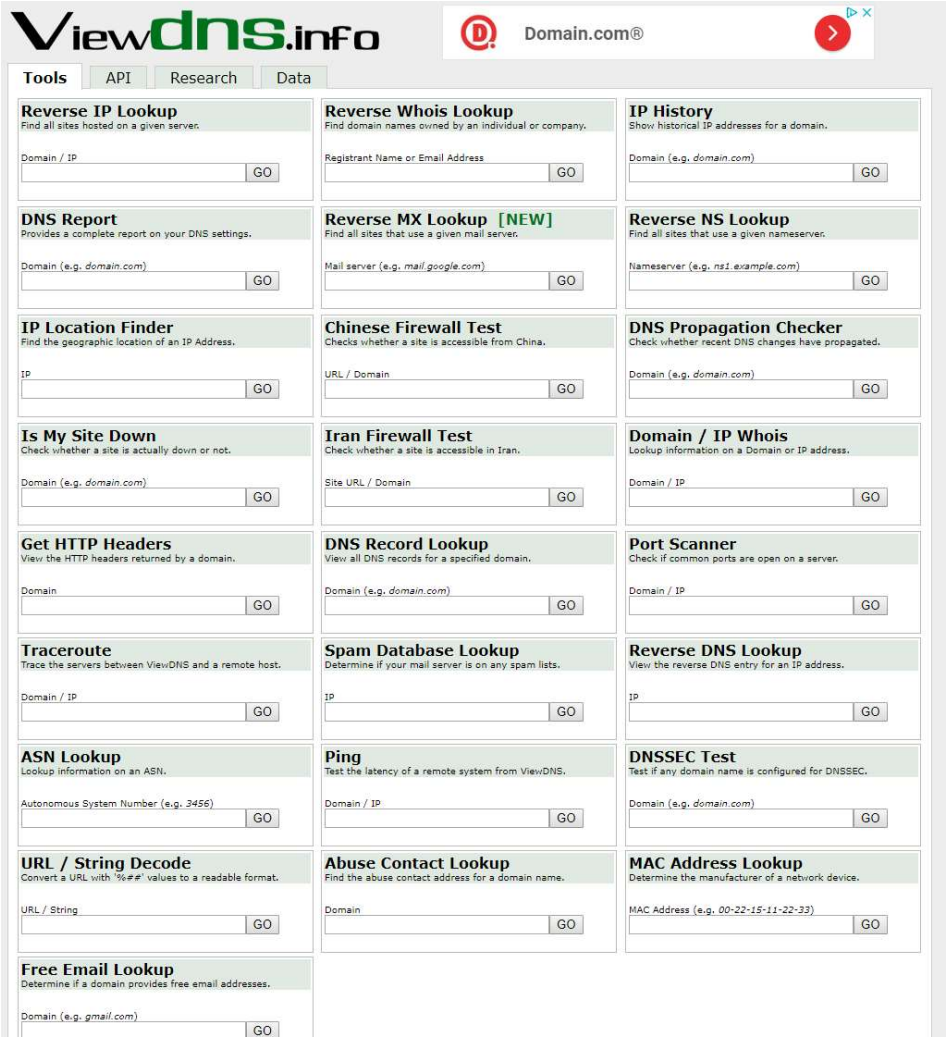
- Address Mapping **records** (A) ...
- IP Version 6 Address **records** (AAAA) ...
- Canonical Name **records** (CNAME) ...
- Host Information **records** (HINFO) ...
- Mail exchanger **record** (MX) ...
- Name Server **records** (NS) ...
- Reverse-lookup Pointer **records** (PTR)

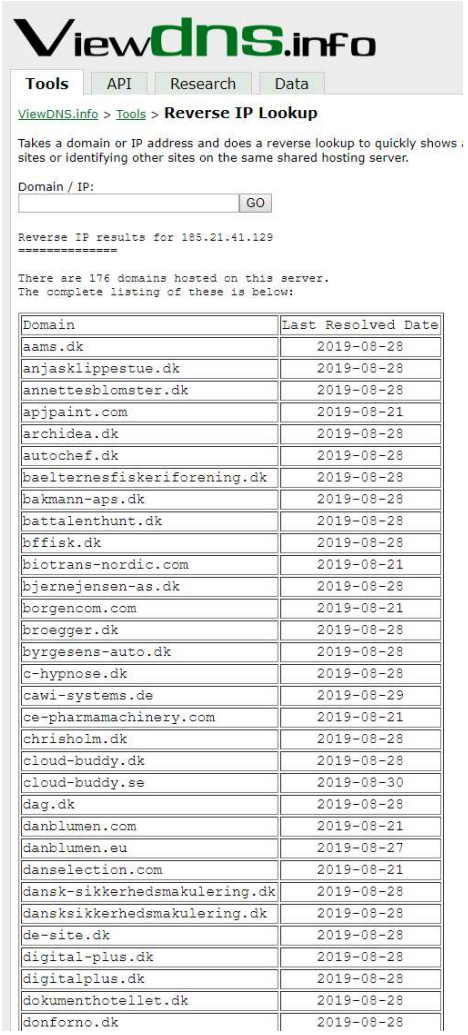
```
┌──(kali㉿kali)-[~]
└─$ nslookup ntnu.no
Server:         158.36.161.21
Address:        158.36.161.21#53

Non-authoritative answer:
Name:   ntnu.no
Address: 129.241.160.102
Name:   ntnu.no
Address: 2001:700:300:6::102
```

General	
FQDN	ntnu.no
Host Name	
Domain Name	ntnu.no
Registry	no
TLD	no
DNS	
IP numbers	2001:700:300:6::102 129.241.160.102
Name servers	ns1.ntnu.no ns2.ntnu.no
Mail servers	mx.ntnu.no

Ip lookup with dns – reverse ip lookup





Domain	Last Resolved Date
aams.dk	2019-08-28
anjasklippestue.dk	2019-08-28
annettesblomster.dk	2019-08-28
apjpaint.com	2019-08-21
archidea.dk	2019-08-28
autochef.dk	2019-08-28
baelternesfiskeriforening.dk	2019-08-28
bakmann-aps.dk	2019-08-28
battalenthunt.dk	2019-08-28
bffisk.dk	2019-08-28
biotrans-nordic.com	2019-08-21
bjernejensen-as.dk	2019-08-28
borgencom.com	2019-08-21
broegger.dk	2019-08-28
byrgesens-auto.dk	2019-08-28
c-hypnose.dk	2019-08-28
cawi-systems.de	2019-08-29
ce-pharmamachinery.com	2019-08-21
chrisholm.dk	2019-08-28
cloud-buddy.dk	2019-08-28
cloud-buddy.se	2019-08-30
dag.dk	2019-08-28
danblumen.com	2019-08-21
danblumen.eu	2019-08-27
danselection.com	2019-08-21
dansk-sikkerhedsmakulering.dk	2019-08-28
dansksikkerhedsmakulering.dk	2019-08-28
de-site.dk	2019-08-28
digital-plus.dk	2019-08-28
digitalplus.dk	2019-08-28
dokumenthotellet.dk	2019-08-28
donforno.dk	2019-08-28

Ip range owners

The *whois* protocol is also used to get the owner of a particular ip range.

The records are stored in different databases according to the continents.

The Norwegian entries are stored in the European database (RIPE NCC)
If we don't know which database to use the general *whois* protocol helps us.

Ip range owners

Who.is says the network region that contains 129.241.160.102 belongs to the RIPE database

IP Whois

```
NetRange:       129.240.0.0 - 129.242.255.255
CIDR:           129.240.0.0/15, 129.242.0.0/16
NetName:        RN-ERX-129-240-0-0
NetHandle:      NET-129-240-0-0-1
Parent:         NET129 (NET-129-0-0-0-0)
NetType:        Early Registrations, Transferred to RIPE NCC
OriginAS:
Organization:   RIPE Network Coordination Centre (RIPE)
RegDate:        2003-01-10
Updated:        2003-06-18
Comment:        These addresses have been further assigned to users in
                the RIPE NCC region.  Contact information can be found in
                the RIPE database at http://www.ripe.net/whois
Ref:            https://rdap.arin.net/registry/ip/129.240.0.0
```

```
inetnum:        129.241.0.0 - 129.241.255.255
netname:        NTNU
descr:          Norwegian University of Scienc
descr:          Hogskoleringen 1
descr:          NO-7491 Trondheim
country:        NO
admin-c:        HA2725-RIPE
tech-c:         NN512-RIPE
status:         LEGACY
mnt-by:         UNINETT-MNT
mnt-lower:      UNINETT-MNT
mnt-irt:        IRT-UNINETT-CERT
created:        2001-12-06T11:14:06Z
last-modified:  2019-12-04T13:04:32Z
source:         RIPE# Filtered
```

Network range examples

Who is the owner of the following ips and how big is the related network range?

- 5.44.65.150
- 195.88.55.16
- 188.44.50.103
- 198.62.101.225
- 194.61.183.124

Hosted websites – Cloud services

- In several cases a website is hosted. That means it is stored on a webserver
  - that does not belong to the target organization
  - which can contain several other websites

In those cases the webpage cannot be attacked or separate permission is needed from the owner of the server computer

Example: elektronikmesse.dk

Finding network ranges

- Search for all domains including second and third level
- Look for the corresponding ips
- Check which database contains the ip owner (*whois*)
- Check the ip ranges (*ripe, arin*, etc…)

Finding network ranges example

- Practice: Find the network ranges of the owner of dn.no
- Solution (demo)
  - dn.no belongs to the **DAGENS NÆRINGSLIV AS**
  - www.dn.no has the ip 87.238.54.132
  - ripe ncc says it is a part of the network range: 87.238.54.128-143
  - the owner of the range is the NHST media group
  - dn.no has the following second level domains: s1,s2,s3,s4, arkiv, multimedia, investor, hotell, idn, ww5, sjakk, pad
  - All the domains are associated with the same ip (87.238.54.132), except the pad.dn.no which is: 87.238.53.121, and the hosted websites (sjakk,)
  - The pad.dn.no is in the range of 87.238.53.0-143

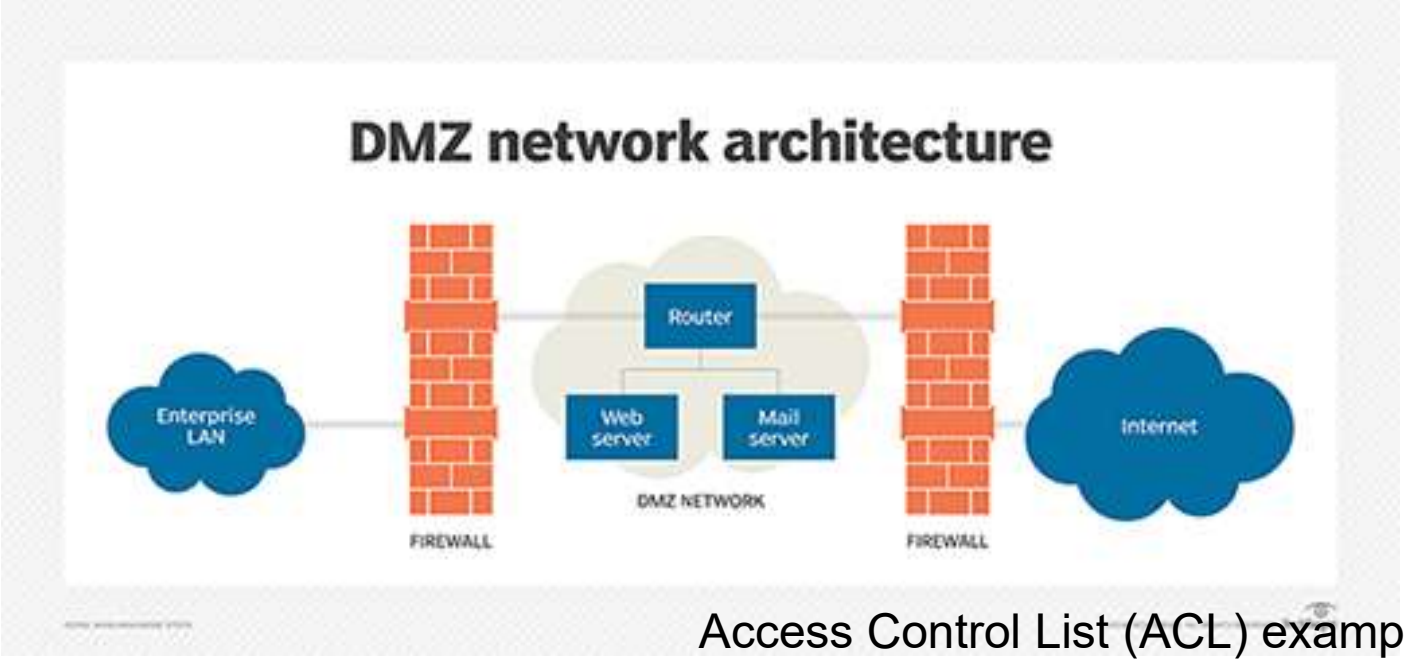
Finding network ranges –reverse whois

With the reverse *whois* service, we can search for domains by providing an email or name.
For example more than 100 domains are associated with the email nhst.no

Finding the range:
dnavis.no -> 87.238.54.132

Domain Name	Creation Date	Registrar
2thefuture.com	2015-04-03	DOMENESHOP AS
2thefuture.no	2013-08-27	
admdir.no	2012-01-25	
aksjespillet.no	2013-08-27	
aquaculturebusiness.com	2006-04-15	DOMENESHOP AS
b2bdagen.no	2013-08-27	
bisbuzz.no	2012-01-25	
businessinfo.no	2017-03-28	
businessnews.no	2012-01-25	
contentshop.no	2012-01-25	
d2.no	2012-01-25	
dagens-naeringsliv.no	2012-01-25	
dagens-naringsliv.no	2012-01-25	
dagensit.no	2013-08-27	
dagensnaeringsliv.no	2012-01-25	
dagensnaringsliv.no	2012-01-25	
dn-dialog.no	2012-01-25	
dn.no	2012-01-25	
dnaktiv.no	2012-01-25	
dnaktivklubb.no	2012-01-25	
dnavis.no	2012-01-25	
dnbo.com	2005-04-14	DOMENESHOP AS
dnbo.no	2012-01-25	
dneiendom.com	2005-11-04	DOMENESHOP AS
dneiendom.no	2012-01-25	
dnenergi.no	2012-01-25	
dngaselle.com	2006-01-26	DOMENESHOP AS
dngaselle.no	2012-01-25	
dngolf.no	2012-01-25	
dngolfen.com	2006-01-26	DOMENESHOP AS
dngolfen.no	2012-01-25	
dnjobb.no	2012-01-25	
dnmarkedspuls.no	2012-01-25	
dnplay.no	2012-01-25	
dnseilcup.com	2006-01-26	DOMENESHOP AS
dnseilcup.no	2012-01-25	
dnservice.no	2012-01-25	
dnspareklubben.com	2006-01-26	DOMENESHOP AS
dnspareklubben.no	2012-01-25	
dntv.no	2012-01-25	
dnvinklubb.no	2012-01-25	

Internal network ip address ranges



Access Control List (ACL) example

Priority/ID	Protocol	Source IP	Src Port	Destination IP	Dst Port	Action
R0	tcp	192.168.1.5	any	*.*.*.*	80	deny
R1	tcp	192.168.1.*	any	*.*.*.*	80	allow
R2	tcp	*.*.*.*	any	172.0.1.10	80	allow
R3	tcp	192.168.1.*	any	172.0.1.10	80	deny
R4	tcp	192.168.1.60	any	*.*.*.*	21	deny
R5	tcp	192.168.1.*	any	*.*.*.*	21	allow
R6	tcp	192.168.1.*	any	172.0.1.10	21	allow
R7	tcp	*.*.*.*	any	*.*.*.*	any	deny
R8	udp	192.168.1.*	any	172.0.1.10	53	allow
R9	udp	*.*.*.*	any	172.0.1.10	53	allow
R10	udp	192.168.2.*	any	172.0.2.*	any	allow
R11	udp	*.*.*.*	any	*.*.*.*	any	deny

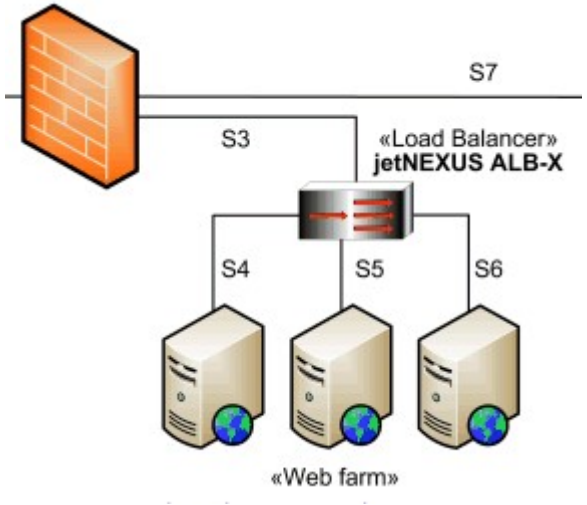
Internal network ips
10.0.0.0/8
192.168.0.0/16
172.16.0.0/12

Domain to ip options

- One domain to one ip

  A webserver with one website
- Multiple domain to one ip

  A web server hosts multiple websites
- One domain to multiple ip
  - Load balancer, cloud service



Robtex

- *Robtex* is used for various kinds of research of IP numbers, Domain names, etc.

Example: dn.no

It belongs to NHST Media Group AS

The network range is:

87.238.32.0/19

87.238.32.0-87.238.63.255

Who is Redpill Linpro?

Robtex

- DNS data is indicated
- Subdomains, similar domains, domains with other TLD

SHARED

Using as CNAME	IP numbers	Sharing IP numbers	Partially sharing IP numbers	Name servers	IP numbers of the name servers	Mail servers	IP numbers of the mail servers
*lantern-static.**dn**.no*	*2a02:c0:207::132*	*avis.**dn**.no*	*cdn.**dn**.no+*	*ns1.**hyp**.net*	*2a01:5b40:ac1::1*	*mx.**nhst**.no*	*62.148.35.170*
1 results shown.	*87.238.54.132*	*www.**dn**.no*	1 results shown.	*ns2.**hyp**.net*	*2a01:5b40:ac2::1*	*mx2.**nhst**.no*	*62.148.35.171*
	2 results shown.	2 results shown.		*ns3.**hyp**.net*	*2a01:5b40:ac3::1*	2 results shown.	2 results shown.
				3 results shown.	*151.249.124.1*		
					151.249.125.2		
					151.249.126.3		
					6 results shown.		

Subdomains/Hostnames

Domains or hostnames one step under this domain or hostname.

*avis.**dn**.no*
*escenicpublish.**dn**.no*
*images.**dn**.no*
*lantern-static.**dn**.no*
*pad.**dn**.no*
*s1.**dn**.no*
*s3.**dn**.no*
*s4.**dn**.no*
*viz.**dn**.no*
*www.**dn**.no*

10 results shown.

Siblings

Siblings are domains or hostnames on the same level, under the same parent level. Not necessarily related in any other way

***dn**.no*
***nd**.no*

2 results shown.

On other TLD:s and domains

This sub section shows this name on other top level domains.

***dn**.com*
***dn**.direct*
***dn**.fi*
***dn**.ht*
***dn**.lt*
***dn**.plus*
***dn**.run*
***dn**.support*
***dn**.tv*
***dn**.zone*

10 results shown.

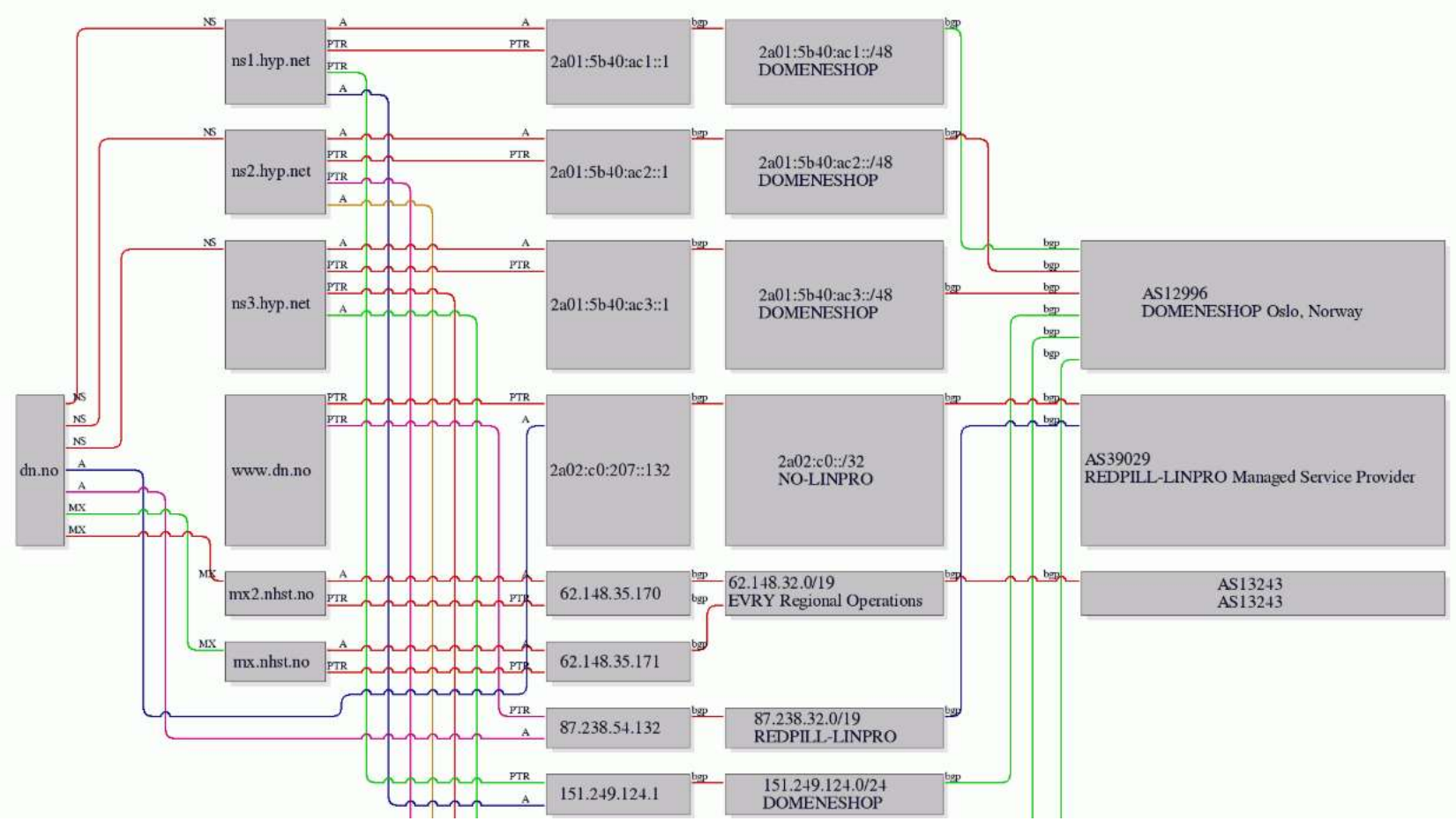
Similar start

This sub section shows this names that begin almost the same.

***nd**.cm*
***nd**.ee*
***nd**.fyi*
***nd**.kg*
***nd**.me*
***nd**.net*
***nd**.org*

Robtex – graph view

It also presents a graph view of the target related ips and ranges



Shodan –IOT device finder

Shodan | Developers | Book | View All...

SHODAN "default password" Explore | Developer Pricing | Enterprise Access | Contact Us

Exploits | Maps

TOTAL RESULTS

66,803

TOP COUNTRIES

Taiwan	9,756
United States	8,274
Brazil	5,833
China	4,033
Iran, Islamic Republic of	3,370

TOP SERVICES

Telnet	17,043
HTTP (8080)	12,302
8081	7,427
Automated Tank Gauge	5,993
HTTPS	3,678

RELATED TAGS: router | default | password

194.177.26.237
PE Service center Maket
Added on 2018-08-26 20:37:31 GMT
Ukraine, Kiev
Details

```
HTTP/1.1 401 N/A
Server: Router Webserver
Connection: close
WWW-Authenticate: Basic realm="TP-LINK Wireless Lite N Router WR740N"
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
  "http://www.w3.org/TR/html4/loose.dtd">
<HTML>
<HEAD>
<TITLE>Login...
```

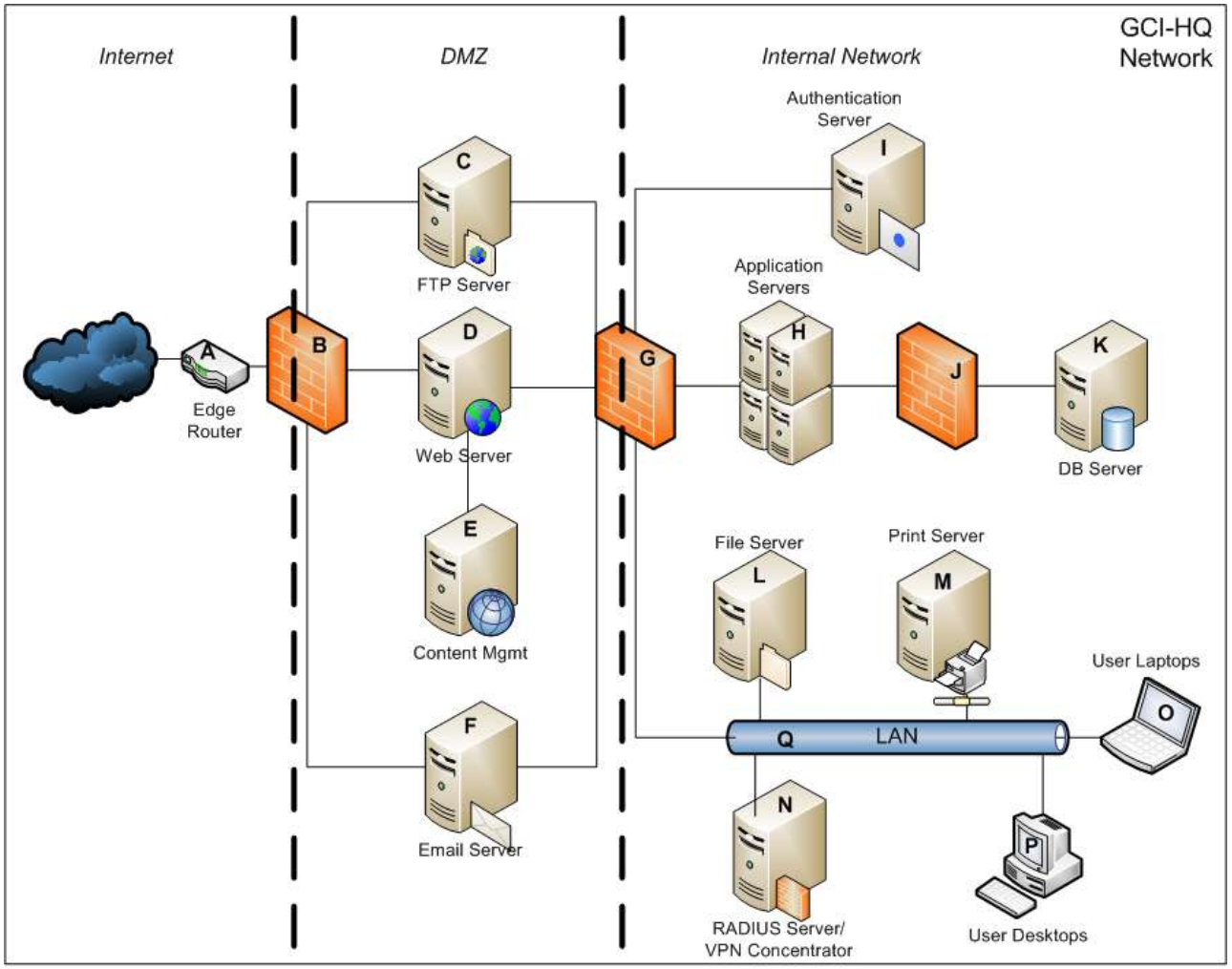
195.140.139.100
kvm139100.profi-server.net
oja.at GmbH
Added on 2018-08-26 20:36:59 GMT
Austria
Details

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 26 Aug 2018 20:29:17 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Keep-Alive: timeout=20
Set-Cookie: iMSCP_Session=1v8c78a4c3umiaoogq16ichj37; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

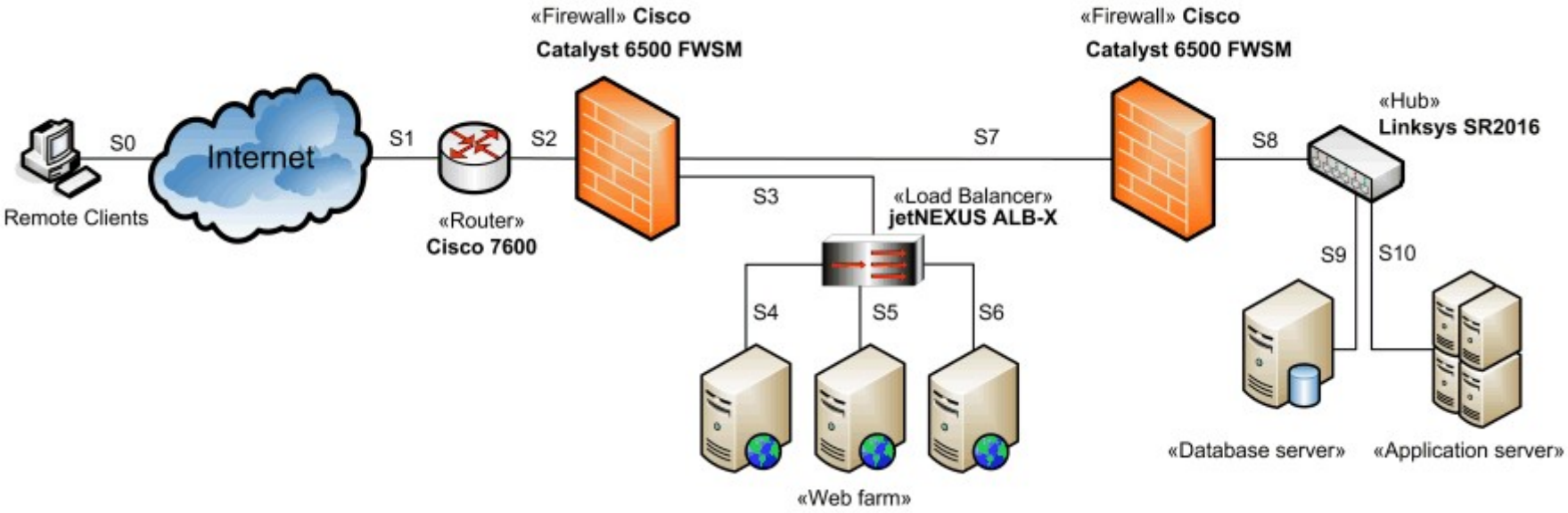
Types of computers in the network

- Server
- Network device (router, switch)
- Firewall (stateless, statefull), Ids, Ips
- Printers
- User desktops
- User laptops
- Mobil devices
- IOTs

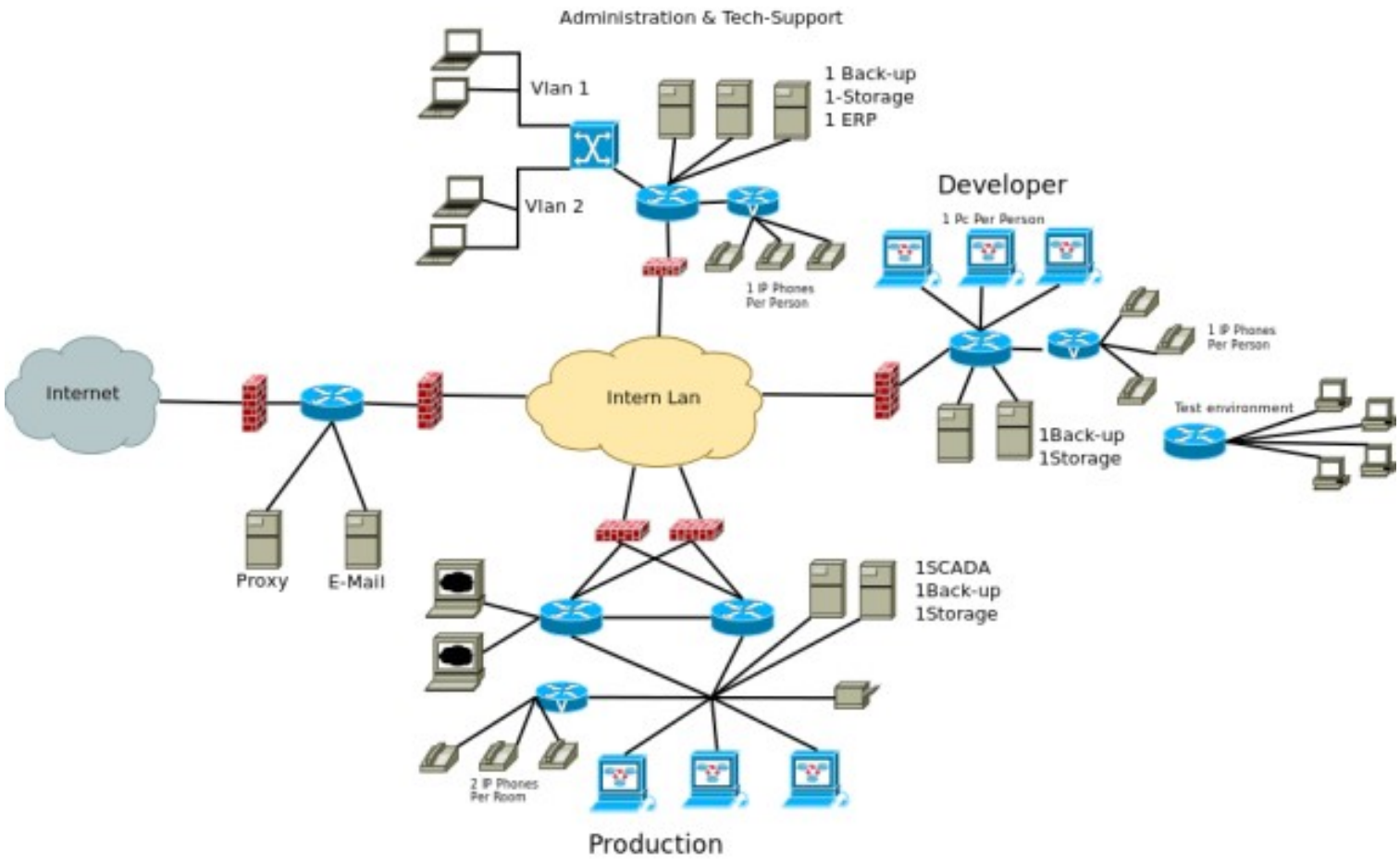
Network layout example 1.



Network layout example 2.



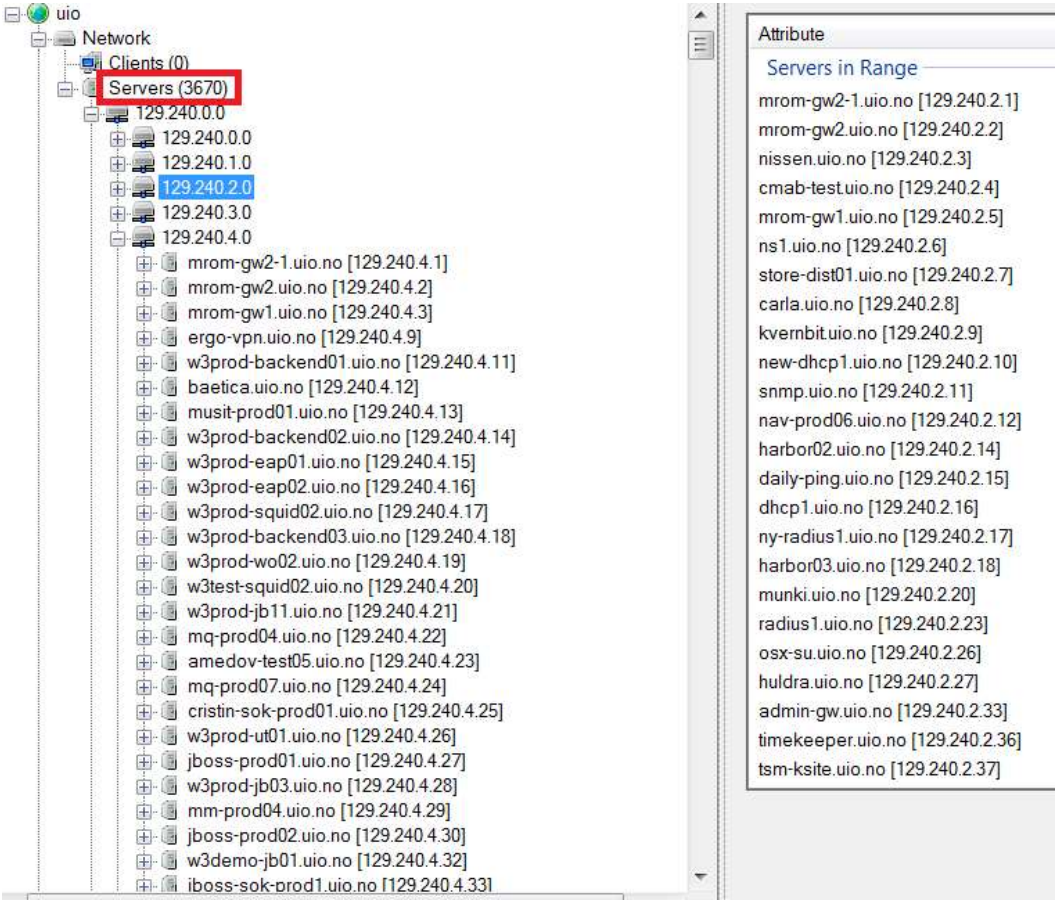
Network layout example 3.



FOCA

Automatically identifies subdomains, servers, ips

- Websearch (google, bing)
- Fingerprinting
- DNS data
- IP Bing
- PTR search
- Shodan & Robtex
- Brute-forcing



End of lecture