SMALL ENTERPRISE LEVEL LAN NETWORK

Small enterprise level LAN network focusing on subnetting, routing, security and internet protocols such as DNS, DHCP and HTTPs based on a cisco packet tracer file

M129_LB3_Bopp

Contents

Changelog

Change	Summary (2-5 words)	Effort
23.01.2024	Created Document structure	10 minutes
24.01.2024	Added content to network, naming convention and introduction	50 minutes

Introduction

Introduction – Tools

Tools	Usage
Draw IO	Creation logical network plan
Cisco Packet Tracer	Creation of functional network
Filius	Creation of simple functional network plan

Introduction – Focus point

The primary objective of this project is to establish a robust enterprise-level network capable of accommodating a workforce ranging from 50 to a maximum of 400 employees. The design of this project is carefully crafted to ensure that, in the event of business expansion, the network can seamlessly adapt to the changes without necessitating a complete restructuring.

A key feature of this network is its future-proof design, ensuring longevity and scalability. Additionally, it facilitates potential upgrades to fibre optic infrastructure, thereby enhancing communication speeds for future requirements.

Another crucial aspect of focus is the implementation of RIP (Routing Information Protocol) for dynamic routing instead of conventional static routing. This dynamic approach enhances the adaptability and efficiency of the network by allowing real-time adjustments to routing configurations.

Introduction – Workforce

Department	Workforce (People)	Network
Organisation	100	SUBNET-ORGANISATION
HR	50	SUBNET-HUMAN-RESSOURCES
IT	75	SUBNET-INFORMATION-TECHNOLOGY

Naming conventions

Naming conventions – Network Devices

Device Full	Device Abbreviation	Brand	DEPARTMENT	Number
ROUTER	RTR	[BRAND]	[DEPARTMENT]	[NUMBER]+1
CORE ROUTER	CRT	[BRAND]	[DEPARTMENT]	[NUMBER]+1
SWITCH	SWT	[BRAND]	[DEPARTMENT]	[NUMBER]+1
CORE SWITCH	CSWT	[BRAND]	[DEPARTMENT]	[NUMBER]+1
ACCESS POINT	ACP	[BRAND]	[DEPARTMENT]	[NUMBER]+1

For [DEPARTMENT] the location abbreviation has to be used always
For [NUMBER]+1 it always has to start with 00[NUMBER]+1
Exception is the Swisscom router see special naming conventions

Naming conventions – Servers

Country Code	Location	ServerType Abbreviation	ServerType Full	Number
CH	[LOCATION]	NTST	NETWORK & STORAGE	[NUMBER]+1
CH	[LOCATION]	WEBS	WEBSERVER	[NUMBER]+1
CH	[LOCATION]	PRNT	PRINTER	[NUMBER]+1

For [LOCATION] the location abbreviation has to be used always
For [NUMBER]+1 it always has to start with 00[NUMBER]+1

Naming conventions – Utility Devices

Device Full	Device Abbreviaiton	Department Abbreviation	BRAND	Number
PRNT	Printer	[DEPARTMENT]	[BRAND]	[NUMBER]+1
NTCM	Netcam	[DEPARTMENT]	[BRAND]	[NUMBER]+1

For [DEPARTMENT] the location abbreviation has to be used always
For [BRAND] the brand abbreviation has to be used always
For [NUMBER]+1 it always has to start with 00[NUMBER]+1

Naming conventions – Clients

Device Full	Device Abbreviation	DEPARTMENT	BRAND	Number
WS	Workstation	[DEPARTMENT]	[BRAND]	[NUMBER]+1
LPT	Laptop	[DEPARTMENT]	[BRAND]	[NUMBER]+1

For [DEPARTMENT] the location abbreviation has to be used always
For [BRAND] the brand abbreviation has to be used always
For [NUMBER]+1 it always has to start with 00[NUMBER]+1

Naming Conventions – Location Code

Location Full	Location Abbreviation
Rüschikon	RKON
Dietlikon	DKON

Naming Conventions – Department

Department Full	Location Abbreviation
Administration	ADM
Information Technology	IT
Human Resources	HR
Organisation	ORG
Garbo	GAB

Note: GARBO is a special naming convention since it isn't a department. It's used for management purposes.

Naming Conventions – Brands

Brand Full	Brand Abbreviation
Cisco	CSC
HP	HP
Dell	DL
Lenovo	LENVO
Hitachi	HTCHI
Xerox	XRX

Naming Conventions – Special

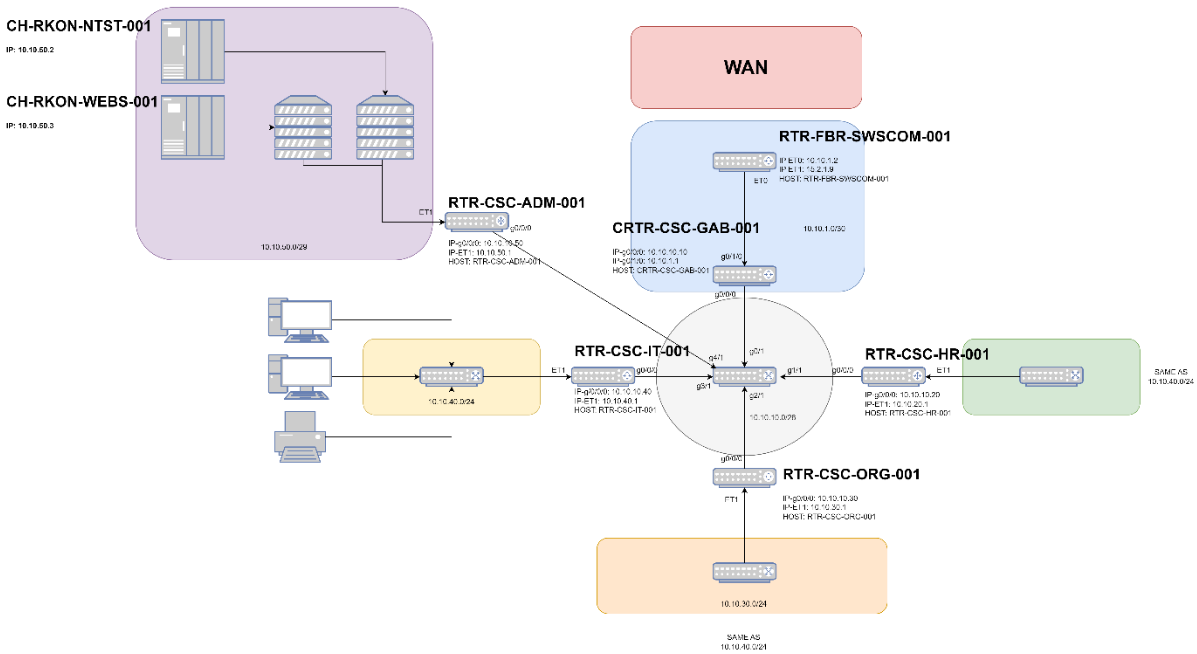
Device Abbreviation	Connection Type Abbreviation	Provider Abbreviation	Number
RTR	**FBR**	**SWSCOM**	**[NUMBER]+1**

Naming Conventions – Connection Types

Connection Type	Connection Type Abbreviation
FibreOptic	FBR
Copper	CPR

Network planning

Network planning – Logical network plan



Network planning – IP addresses – Network devices

Device	IP-address I0	IP-address I1	CIDR I0	CIDR I1	MAC-I0	MAC-I1
RTR-CSC-SWSCOM	10.10.1.2	15.23.68.222	/30	/0	0040.0B84.35AA	0001.4390.D8CC
CRTR-CSC-GAB	10.10.10.10	10.10.1.1	/28	/29	00D0.FFA1.9038	00D0.97D1.ED6B
RTR-CSC-HR	10.10.10.20	10.10.20.1	/28	/24	0006.2A77.3C81	000C.CF2A.22C0
RTR-CSC-ORG	10.10.10.30	10.10.30.1	/28	/24	0060.7093.446D	0006.2A3D.DE05
RTR-CSC-IT	10.10.10.40	10.10.40.1	/24	/24	000C.CF8C.703D	000A.F374.BC02
RTR-CSC-ADM	10.10.10.50	10.10.50.1	/28	/29	0001.9793.1DE1	000C.CFB2.467A

All routers interfaces that are facing outwards meaning into the GAB-RTR are in the 10.10.10.0/28 Network you can also verify this in the below mentioned subnet addressing table. The inward facing router interfaces inherit the IP ending of their outwards facing router interfaces. Meaning the router with the outwards facing interface with the IP 10.10.10.20 will have the inward facing interface with the IP 10.10.10.20.1

I also purposely used different CIDRs to not waste any space, however the Working Environment subnet stay /24 since they have different devices in them that I want to differentiate.

Network planning – IP addresses – Servers

Server	IP-address	MAC-address	packages
CH-RKON-NTWK-001	10.10.50.2	0001.4259.42A8	DNS, Email
CH-RKON-WEBS-001	10.10.50.3	0060.70DC.BC5B	APACHE2

All servers are in the administrative subnet or in the ADM-SUBNET. The Servers are in the ADM-Subnet since they need higher privileges and work on an administrative level.

Network planning – IP addresses – Hosts

Group	Reserved IP Range	IP assigning
Devices (Printer, Smart Lamps, etc.)	x.x.x.10 – x.x.x.40	Static
Hosts	x.x.x.100 – x.x.x.220	DHCP
Maintenance	x.x.x.220 – x.x.x.254	Static

In the network setup, hosts are snagging their IPs via DHCP. As you've spotted, we've mapped out some nifty IP ranges. Now, you might wonder, "Where's the DHCP server in the logical network plan?" Good catch, my friend. Intentionally, there's no central DHCP server in the mix. Why, you ask? Relying solely on one server is a bit like walking on thin ice. If it decides to take a break – be it for maintenance or an impromptu implosion – we're in a bind. That's precisely why I've opted for the reliability of multiple dedicated DHCP servers instead of a high-risk low-cost solution with multiple relays. Gotta keep it robust and foolproof.

Network planning – DHCP – IP Pools

NAME	ROUTER	POOL RANGE
DHCP-ORG	RTR-CSC-ORG-001	10.10.30.100 – 10.10.30.220
DHCP-IT	RTR-CSC-IT-001	10.10.40.100 – 10.10.40.220
DHCP-HR	RTR-CSC-HR-001	10.10.20.100 – 10.10.20.220

Network planning – Subnets

Subnet	CIDR	Network	Description	Colour
GAB-Outgoing	/30	10.10.1.0	Connector network to WAN	
GAB-RTR	/28	10.10.10.0	Used for Routers.	
HR	/24	10.10.20.0	For people working in HR department.	
ORG	/24	10.10.30.0	For people working in the organisation department.	
IT	/24	10.10.40.0	For people working in the IT department.	
ADM	/29	10.10.50.0	For devices that are used for administrative purposes or operate at a higher level.	

Hardware

Hardware – Network Devices

Device	Brand	Device Model	Price CHF	Modules (add.)
Router	CSC	CISCO2911SEC	1050	HWIC-1GE-SFP GLC-LH-SMD
Core Switch	CSC	PT-SWITCH-EMPTY	--------	PT-SWITCHNM-1FGE
Switch	CSC	CISCO2950T-24	400	--------------------------
Firewall	CSC	ASA5506-SEC-K9	660	--------------------------
Access point	CSC	Access Point PT	-------------	--------------------------

I used the **HWIC-1GE-SFP** and the **GLC-LH-SMD** to receive and send over fibreoptic wires. These are all connected to the **PT-SWITCH-EMPTY** to the **PT-SWITCHNM-1FGE** This allows gigabit telecommunication in the network. To connect them I used fibre cables. Note that fibre cables only get used in the **GAB-RTR** Subnet.

For the use of Hardware, I chose a simple core switch which I can customize without having any superfluous interfaces. I needed to customize it since normal switches don't natively support fibre optic connectivity. For the Switches inside each of the subnets I used a 24-Port switch which isn't that expensive for a small enterprise (see prise above) another alternative would be to use a **3650-24PS Switch** now you might have noticed that the switch I just mentioned begins with 3 this is because it's a layer 3 switch which supports stacking, stacking is when two or more switches get logically combined into one big switch. **650** is the model of layer 3 switch. And **24PS** is the number of ports the switch possesses.

Hardware – Server

Device	Brand	Device Model	Price CHF	Modules (add.)
Webserver	HP	Server DL360 G9 FF	3460	--------------------------
Storagesever	HTCHI	VSP 990E	-------------	--------------------------
Printerserver	HP	Server DL360 G9 FF	3460	--------------------------

I decided to use these hardware specs as a server because that's what we use in our family company.

Hardware – Hosts

Device	Brand	Device Model	Price CHF	Modules (add.)
WS-ADM	HP	HP Pro DM 400 G9	924	--------------------------
WS-HR	HP	HP Pro DM 400 G9	924	--------------------------
WS-IT	HP	HP Pro DM 400 G9	924	--------------------------
WS-ORG	HP	Pro Tower 400 G9	983	--------------------------

Hardware – Hosts – Special- IT

Device	Brand	Device Model	Price CHF	Use
WS	DL	OptiPlex 9070 Plus	876	LAB USE
LPT	LENVO	ThinkPad E14 Gen 5	899	LAB USE

IP Associating

IP Associating – Scheme

Network	Colour	Associating Scheme	Range (Hosts)
ORG		DHCP	x.x.x.100 – x.x.x.220
HR		DHCP	x.x.x.100 – x.x.x.220
IT		DHCP	x.x.x.100 – x.x.x.220
ADM		Static	x.x.x.100 – x.x.x.220

See network planning – IP addresses – Hosts for more information.

IP Associating – Servers (Util)

Server	Description	IP-Address	Network
CH-RKON-NTST-001	DNS and Storage Server	10.10.50.2	SUBNET-ADM
CH-RKON-WEBS-001	Webserver	10.10.50.3	SUBNET-ADM

IP Associating – Servers (DHCP)

Server	Description	IP-Address	Network
DHCP-ORG	DHCP for ORG subnet	10.10.30.**10**	SUBNET-ORG
DHCP-IT	DHCP for IT subnet	10.10.40.**10**	SUBNET-IT
DHCP-HR	DHCP for HR subnet	10.10.20.**10**	SUBNET-HR

IP Associating - Clients – IT

Device Name	Description	IP-Address	Network
WS-IT-HP-001	HP Pro DM 400 G9	DHCP	SUBNET-IT
WS-IT-HP-002	HP Pro DM 400 G9	DHCP	SUBNET-IT
WS-IT-HP-003	HP Pro DM 400 G9	DHCP	SUBNET-IT

IP Associating - Clients – HR

Device Name	Description	IP-Address	Network
WS-HR-HP-001	HP Pro DM 400 G9	DHCP	SUBNET-HR
WS-HR-HP-002	HP Pro DM 400 G9	DHCP	SUBNET-HR
WS-HR-HP-003	HP Pro DM 400 G9	DHCP	SUBNET-HR

IP Associating - Clients – ORG

Device Name	Description	IP-Address	Network
WS-ORG-HP-001	HP Pro DM 400 G9	DHCP	SUBNET-ORG
WS-ORG-HP-002	HP Pro DM 400 G9	DHCP	SUBNET-ORG
WS-ORG-HP-003	HP Pro DM 400 G9	DHCP	SUBNET-ORG

Realization

Realization – Routing Table – CRTR-CSC-GAB-001

Network	Subnet mask	Next Hop
10.10.50.0	255.255.255.248	10.10.10.5
10.10.40.0	255.255.255.0	10.10.10.4
10.10.30.0	255.255.255.0	10.10.10.3
10.10.20.0	255.255.255.0	10.10.10.2
0.0.0.0	0.0.0.0	10.10.1.2

Realization – Routing Table – CRTR-CSC-HR-001

Network	Subnet mask	Next Hop
10.10.50.0	255.255.255.248	10.10.10.5
10.10.40.0	255.255.255.0	10.10.10.4
10.10.30.0	255.255.255.0	10.10.10.3
10.10.1.0	255.255.255.252	10.10.10.1
0.0.0.0	0.0.0.0	10.10.10.1

Realization – Routing Table – CRTR-CSC-ORG-001

Network	Subnet mask	Next Hop
10.10.50.0	255.255.255.248	10.10.10.5
10.10.40.0	255.255.255.0	10.10.10.4
10.10.20.0	255.255.255.0	10.10.10.2
10.10.1.0	255.255.255.252	10.10.10.1
0.0.0.0	0.0.0.0	10.10.10.1

Realization – Routing Table – CRTR-CSC-IT-001

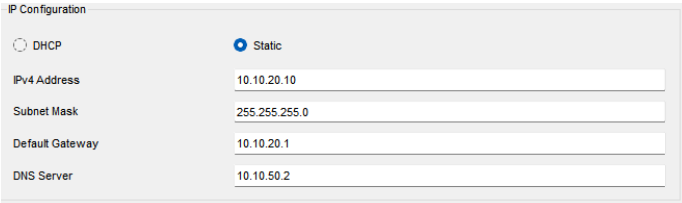
Network	Subnet mask	Next Hop
10.10.50.0	255.255.255.248	10.10.10.5
10.10.30.0	255.255.255.0	10.10.10.3
10.10.20.0	255.255.255.0	10.10.10.2
10.10.1.0	255.255.255.252	10.10.10.1
0.0.0.0	0.0.0.0	10.10.10.1

Realization – Routing Table – CRTR-CSC-ORG-001

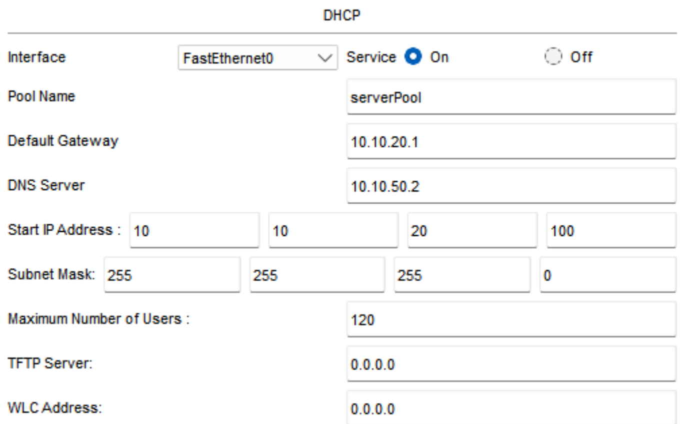
Network	Subnet mask	Next Hop
10.10.40.0	255.255.255.0	10.10.10.4
10.10.30.0	255.255.255.0	10.10.10.3
10.10.20.0	255.255.255.0	10.10.10.2
10.10.1.0	255.255.255.252	10.10.10.1
0.0.0.0	0.0.0.0	10.10.10.1

Realization – DHCP – DHCP-HR

IP configuration

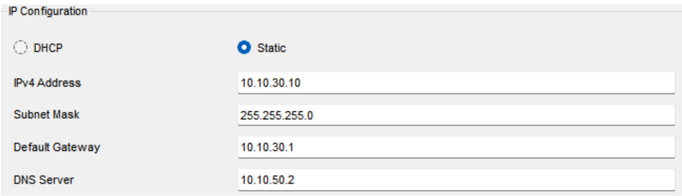


DHCP configuration

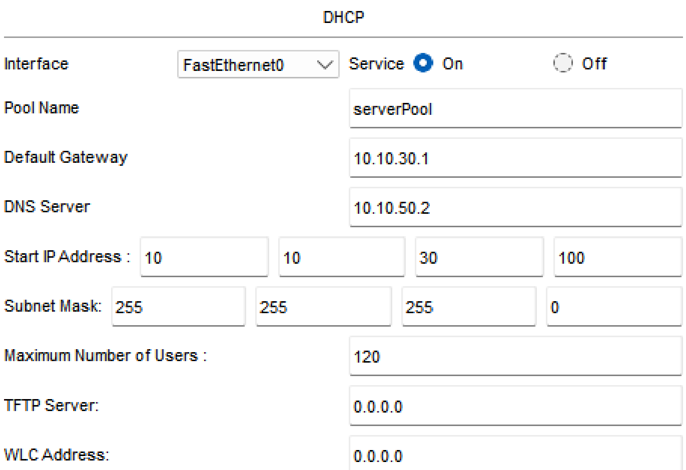


Realization – DHCP – DHCP-ORG

IP configuration

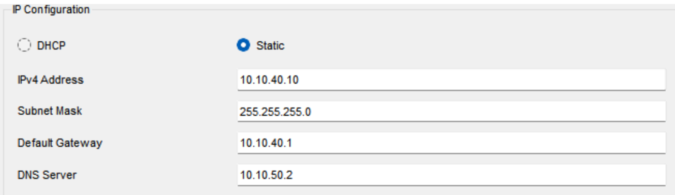


DHCP configuration

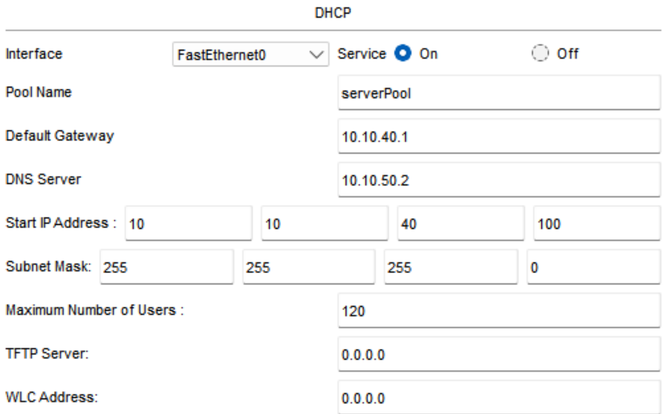


Realization – DHCP – DHCP-IT

IP configuration



DHCP configuration



Realization – DNS – DNS Server Configuration

IP Configuration

IPv4 Address	Subnet Mask	Default Gateway	DNS Server
10.10.50.2	255.255.255.248	10.10.50.1	10.10.50.2

DNS Entries

No.	Name	Type	Detail
0	Intranet.gab.ch	A Record	10.10.50.3

Realization – Email – Email Server Configuration

IP Configuration

IPv4 Address	Subnet Mask	Default Gateway	DNS Server
10.10.50.2	255.255.255.248	10.10.50.1	10.10.50.2

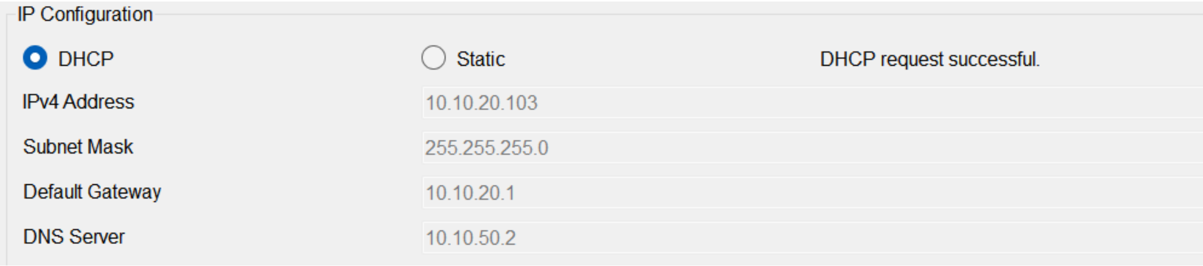
User Setup

Domain Name	User	Password	Email
Gab.ch	Rayan.bopp	abcdu12surkdus	Rayan.bopp@gab.ch
Gab.ch	Miguel.juan.carlitos	abcdu12surkduss	miguel.juan.carlitos@gab.ch

Testing

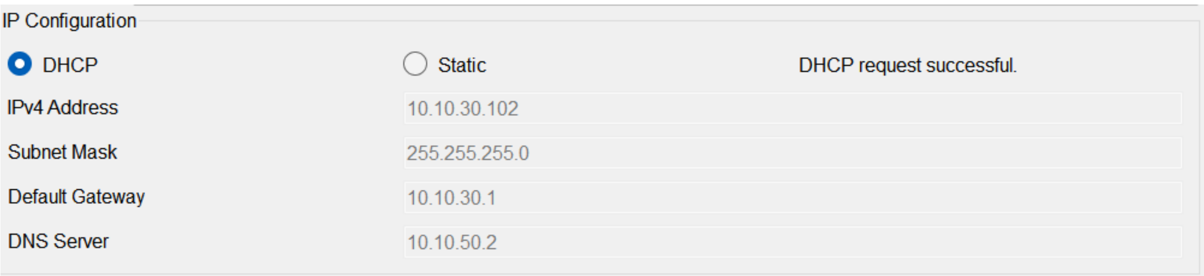
Testing – DHCP – DHCP HR

I will only test one of the three workstations I've put in the subnet, because if that works the others will work as well.



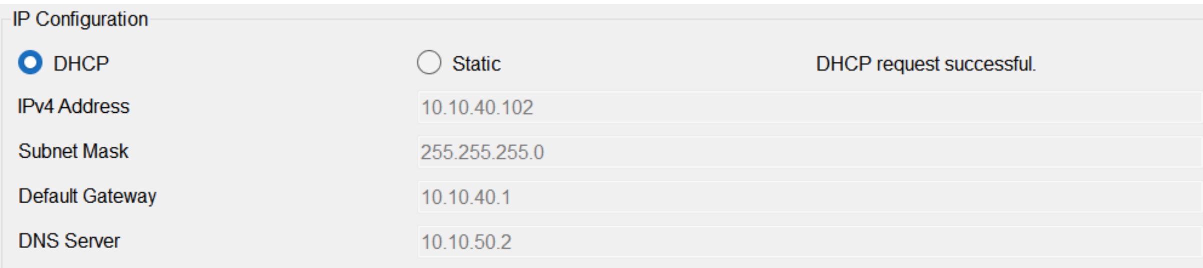
Testing – DHCP – DHCP ORG

I will only test one of the three workstations I've put in the subnet, because if that works the others will work as well.



Testing – DHCP – DHCP IT

I will only test one of the three workstations I've put in the subnet, because if that works the others will work as well.



Testing – DHCP – Conclusion

Upon thorough examination, it becomes evident that all configurations have been meticulously set up, aligning seamlessly with the intended specifications, and the system operates flawlessly, precisely as designed, and expected.

Testing – Email – Communication

As stated before, I've added two users that can use the email service:

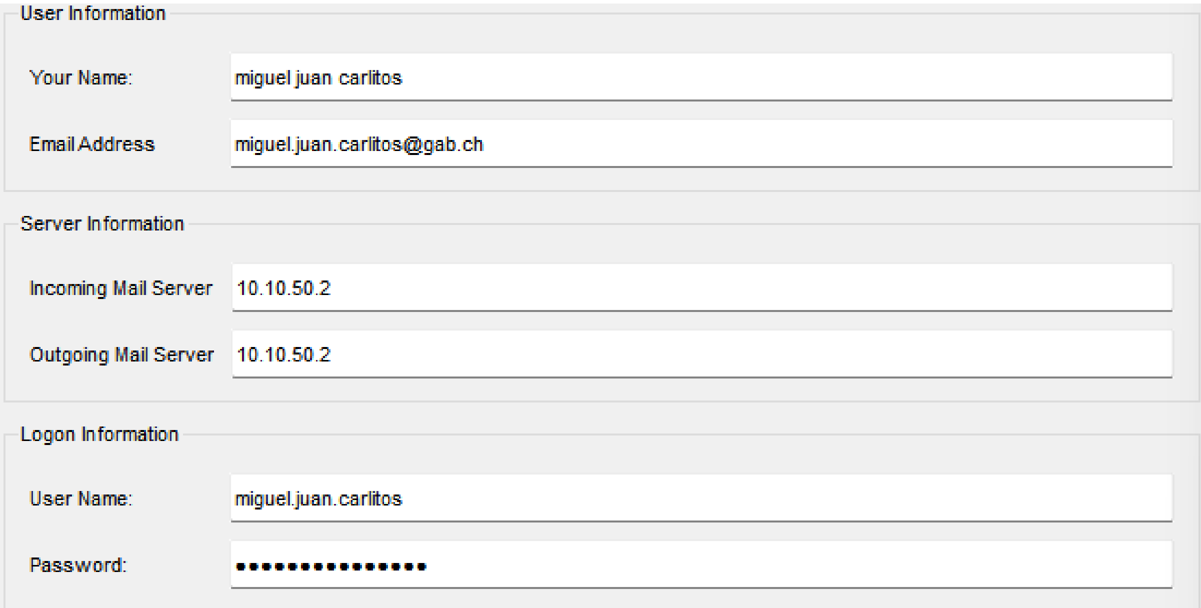
Domain Name	User	Password	Email
Gab.ch	Rayan.bopp	abcdu12surkdus	Rayan.bopp@gab.ch
Gab.ch	Miguel.juan.carlitos	abcdu12surkduss	miguel.juan.carlitos@gab.ch

These users can then use the Workstations to communicate with each other. For this test I'll assign them different workstations in different subnets.

PC-Name	IP-address	Subnet	Assigned user
WS-HR-HP-002	10.10.20.103	SUBNET-HR	Miguel juan carlitos
WS-IT-HP-001	10.10.40.101	SUBNET-IT	Rayan Bopp

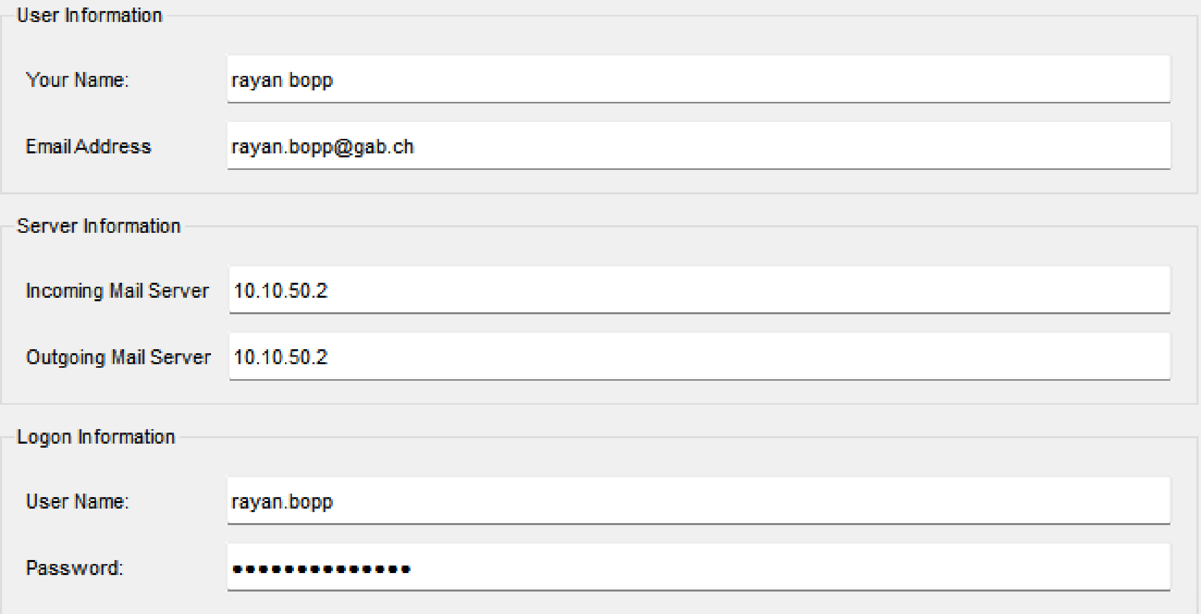
Testing – Email – Mail Client Configuration – Miguel Juan Carlitos

Now I must configure the mail client to use the mail server to communicate inside the network. I'll start with the mail client of Miguel Juan Carlitos:



Testing – Email – Mail Client Configuration – Rayan Bopp

Now having configured Miguel Juan Carlitos mail client it's time to configure my mail client.



Testing – Email – Mail Client Configuration – Explanation

Alright, let me break it down for you. I've set up the email clients to exclusively handle internal communication, meaning they'll only deal with messages within our network. This is achieved by designating our internal mail server at 10.10.50.2 as both the incoming and outgoing server.

Now, suppose you need to send emails externally. In that case, you can set up a proxy, let's call it ProxyX, with the LAN IP 10.10.50.4. This proxy will have a reverse entry pointing outward, acting as a middleman between your internal network and the external world. This way, the proxy facilitates communication outside our network.

For example, if you want to send an email to an external contact, the email client sends the message to ProxyX (10.10.50.4), and then ProxyX forwards it to the external recipient. On the receiving end, incoming rules can be configured to allow emails from the wide area network (WAN) to be received by the email clients in the local area network (LAN) with the mail server's IP (10.10.50.2). This ensures smooth communication between internal and external sources.

Testing – Email – Send and Recieve

Now with all the mail clients configured let's send out a test email. This test email will be sent from Rayan Bopp and be sent to Miguel Juan Carlitos. It will have the following contents:

Hello this is a test.

If you've received this test email the mail server and mail client have been configured correctly.

Please make sure to respond to this email with the following response:

Hello this is a reply

If you've received this reply email the email server and mail client have been configured correctly.

Thank you for your time

Email sent confirmation for Rayan Bopp:

```
Sending mail to miguel.juan.carlitos@gab.ch , with subject : Test ..
Mail Server: 10.10.50.2
Send Success.
```

Receive Email confirmation for Miguel Juan Carlitos:

```
Receiving mail from POP3 Server 10.10.50.2
Receive Mail Success.
```

	From	Subject	Received
1	rayan.bopp@gab.ch	Test	Fri Feb 2 2024 17:02:48

Test
rayan.bopp@gab.ch
Sent : Fri Feb 2 2024 17:02:48

Hello this is a test.
If you've received this test email the mail server and mail client have been configured correctly.
Please make sure to respond to this email with the following response:
Hello this is a reply
If you've received this reply email the email server and mail client have been configured correctly.
Thank you for your time

Send Email confirmation for Miguel Juan Carlitos:

```
Sending mail to rayan.bopp@gab.ch , with subject : RE: Test ..
Mail Server: 10.10.50.2
Send Success.
```

Receive Emial confirmation for Rayan Bopp:

Receiving mail from POP3 Server 10.10.50.2
Receive Mail Success.

	From	Subject	Received
1	miguel.juan.carlitos@gab.ch	RE: Test	Fri Feb 2 2024 17:04:35

RE: Test
miguel.juan.carlitos@gab.ch
Sent : Fri Feb 2 2024 17:04:35

Hello this is a reply
If you've received this reply email the email server and mail client have been configured correctly.

Subject : Test
From : rayan.bopp@gab.ch
Sent : Fri Feb 2 2024 17:02:48

Testing – Email – Conclusion

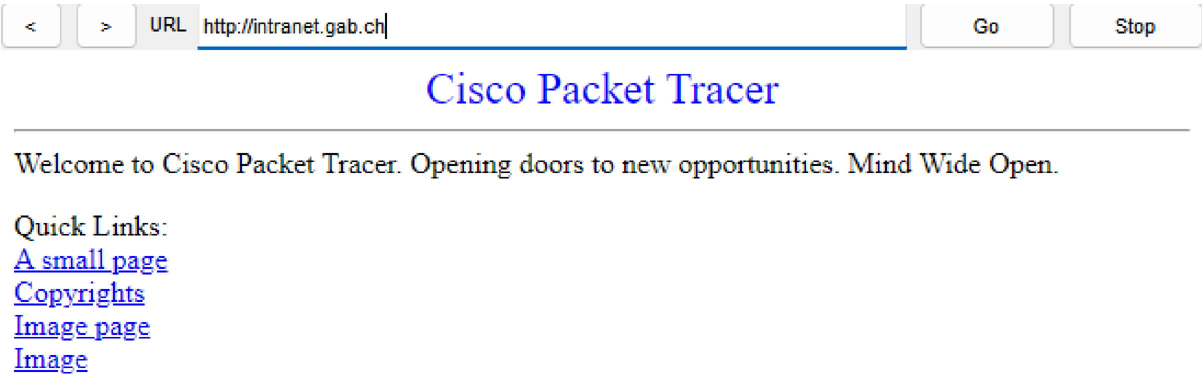
All test scenarios were executed successfully, confirming the efficacy of the configured system. Internal communication pathway are functional.

Testing – DNS – HTTP Request

To test the DNS-Entries we must make a request for one of these DNS-Entries, so here I have made an A-Record “intranet.gab.ch” pointing at the ipv4-address 10.10.50.3.

No.	Name	Type	Detail
0	intranet.gab.ch	A Record	10.10.50.3

This has been performed from Miguel Juan Carlitos Workstation



Testing – DNS – Conclusion

All test scenarios were executed successfully, confirming the efficacy of the configured system.

Testing – Ping test scenarios – Internal communication

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC9	PC2	ICMP		0.000	N	0	(edit)	(delete)
	Successful	CH-RK...	PC9	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC1	PC9	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC2	PC1	ICMP		0.000	N	3	(edit)	(delete)

Testing- Ping test scenarios – Conclusion

All tests have been successfully executed meaning that all the routing table entries are correctly implemented.

Technical Jargon

Technical Jargon – Copper Cables

Copper cables, the unsung heroes of data transmission, have played a pivotal role in shaping the technological landscape. Introduced in the early 20th century, these cables revolutionized communication, laying the foundation for today's interconnected world.

- **Inception:** The use of copper for electrical conductivity dates to the 19th century, but it was in the 1920s that the first practical applications of copper cables for telecommunication emerged.
- **Milestones:** The evolution of copper cables witnessed significant milestones, including the introduction of twisted pair cables in the 1930s and the development of coaxial cables in the 1940s.

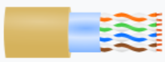
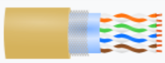
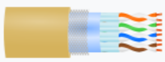
Technical Jargon – Copper Cables – Versions

The journey of copper cables is marked by various versions, each contributing to enhanced data transmission capabilities.

- **First Generation (1920s):** Basic copper wires facilitated voice communication.
- **Second Generation (1930s):** Twisted pair cables improved signal quality and reduced interference.
- **Third Generation (1940s):** Coaxial cables allowed for higher bandwidth, enabling the transmission of television signals.

Technical Jargon – Copper Cables – Types

Common industry nomenclature for cable construction types

Industry abbreviations	ISO/IEC 11801 designation[A]	Cable shielding	Pair shielding	Illustration
UTP, TP	U/UTP	None	None	
FTP, STP, ScTP	F/UTP	Foil	None	
STP, ScTP	S/UTP	Braiding	None	
SFTP, S-FTP, STP	SF/UTP	Braiding and Foil	None	
STP, ScTP, PiMF	U/FTP	None	Foil	
FFTP, STP	F/FTP	Foil	Foil	
SSTP, SFTP, STP, STP PiMF	S/FTP	Braiding	Foil	
SSTP, SFTP, STP	SF/FTP	Braiding and Foil	Foil	

A. ^ The code before the slash designates the shielding for the cable itself, while the code after the slash determines the shielding for the individual pairs:

U – unshielded
F – foil shielding
S – screened shielding (outer layer only)
TP – twisted pair
TQ – twisted pair, individual shielding in quads

Standards

Standard types of twisted pair cabling

Name	Typical construction	Bandwidth	Applications	Notes
Level 1		400 kHz	Telephone and modem lines	Not described in EIA/TIA recommendations. Unsuitable for modern systems.[15]
Level 2		4 MHz	Older terminal systems, e.g. IBM 3270	Not described in EIA/TIA recommendations. Unsuitable for modern systems.[15]
Cat 3	UTP[16]	16 MHz[16]	10BASE-T, 100BASE-T4[16]	Described in EIA/TIA-568. Unsuitable for speeds above 16 Mbit/s. Now mainly for telephone cables.[16]
Cat 4	UTP[16]	20 MHz[16]	16 Mbit/s Token Ring[16]	Not commonly used[16]
Cat 5	UTP[16]	100 MHz[16]	100BASE-TX, 1000BASE-T[16]	Common for current LANs. Superseded by Cat 5e, but most Cat 5 cables meet Cat 5e standards.[16] Limited to 100 m between equipment.
Cat 5e	UTP,[16] F/UTP, U/FTP[17]	100 MHz[16]	1000BASE-T, 2.5GBASE-T[16]	Enhanced Cat 5. Common for current LANs. Same construction as Cat 5, but with better testing standards.[16] Limited to 100m between equipment.
Cat 6	UTP,[16] F/UTP, U/FTP[18]	250 MHz[16]	5GBASE-T, 10GBASE-T	ISO/IEC 11801 2nd Ed. (2002), ANSI/TIA 568-B.2-1. Limited to 55 m distance at 10GBASE-T
Cat 6A	UTP, F/UTP, U/FTP, S/FTP	500 MHz	5GBASE-T, 10GBASE-T	Improved standards, tested to 500 MHz. Full 100 m distance at 10GBASE-T ISO/IEC 11801 2nd Ed. Am. 2. (2008), ANSI/TIA-568-C.1 (2009)
Cat 7	S/FTP, F/FTP	600 MHz	?	ISO/IEC 11801 2nd Ed. (2002). Only with GG45 or TERA connectors. It is not recognized by the EIA/TIA.
Cat 7_A	S/FTP, F/FTP	1 GHz	?	ISO/IEC 11801 2nd Ed. Am. 2. (2008). Only with GG45 or TERA connectors. It is not recognized by the EIA/TIA.
Cat 8.1	F/UTP, U/FTP	2 GHz	25GBASE-T, 40GBASE-T	ANSI/TIA-568-C.2-1, ISO/IEC 11801-1:2017
Cat 8.2	S/FTP, F/FTP	2 GHz	25GBASE-T, 40GBASE-T	ISO/IEC 11801-1:2017

Technical Jargon – Fibre Optic Cables

Fiber optic cables, often referred to as optical fibers, are a cornerstone in modern telecommunications and data transmission systems. They utilize the principles of total internal reflection to transmit data in the form of light pulses, enabling high-speed and long-distance communication.

Historical Evolution:

- **1960s:** The concept of fiber optics originated with research in the 1960s, pioneered by Corning Glass Works and Bell Labs.
- **1970s:** Practical applications began to emerge, with the first experimental fiber optic communication system deployed in 1977.
- **1980s:** Mass production and commercialization gained momentum, marking a significant shift in global communication infrastructure.

RFC References:

The detailed specifications and standards for fiber optic cables are outlined in various Request for Comments (RFC) documents. Notable references include:

- **RFC 791 - "Internet Protocol" (1981):** Initial integration of fiber optics in the emerging Internet infrastructure.
- **RFC 2474 - "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers" (1998):** Evolution of fiber optic usage in enhancing Quality of Service (QoS).
- **RFC 4950 - "ICMP Extensions for Multiprotocol Label Switching" (2007):** Illustrates the integration of fiber optics in advanced networking protocols.

Technical Jargon – Fibre Cables – Versions

- **Single-mode (SM) Fibers:** Optimized for long-distance communication with a single, narrow optical mode.
- **Multi-mode (MM) Fibers:** Suited for shorter distances with multiple optical modes.

Technical Jargon – Fibre Cables – Types

- **Standard Single-mode Fiber (G.652):** Widely used for long-haul telecommunications.
- **Dispersion-Shifted Fiber (G.653):** Addresses signal distortion issues over extended distances.
- **Non-Zero Dispersion-Shifted Fiber (G.655):** Enhances performance by mitigating dispersion effects.
- **Multi-mode Fiber (OM1 to OM5):** Varying core sizes catering to different distance requirements.

Technical Jargon – Fibre Cables – Functionality

- **Data Transmission:** Fiber optic cables transmit data through the propagation of light signals, offering high bandwidth and low signal attenuation.
- **Applications:** Widely employed in telecommunications, internet infrastructure, and networking environments.
- **Advantages:** Immunity to electromagnetic interference, high data transfer rates, and low latency.

Technical Jargon – Switches

- **Switch:** A network switch, also known as a switching hub, is a networking device that operates at Layer 2 (Data Link Layer) of the OSI model. It facilitates communication within a local area network (LAN) by using MAC addresses.
- **Layer 2 Switch:** This type of switch operates at the Data Link Layer, making decisions based on MAC addresses. It is proficient in creating and managing VLANs, enhancing network segmentation.
- **Layer 3 Switch:** Combining the functionalities of a traditional switch and a router, a Layer 3 switch operates at both Layer 2 and Layer 3, allowing for IP routing within the network.

Historical Dates and RFC:

- The concept of network switches was introduced in the late 1970s with the advent of Ethernet technology.
- The IEEE 802.1Q standard, defined in 1998, introduced VLAN support, a crucial aspect of switch functionality.
- The Spanning Tree Protocol (STP) was standardized in IEEE 802.1D in 1990, ensuring loop-free topology.
- Power over Ethernet (PoE) specifications are defined in the IEEE 802.3af and 802.3at standards, ratified in 2003 and 2009, respectively.
- The basics of switch functionality are outlined in various RFCs, with RFC 826 addressing ARP (Address Resolution Protocol), a fundamental aspect of switch operation.

Technical Jargon – Switches – Functionality

- **Forwarding:** Switches use MAC addresses to forward data frames between devices within the same network. This is done by maintaining a MAC address table, also known as a content addressable memory (CAM) table.
- **Broadcast Storm Prevention:** Switches mitigate network congestion by intelligently forwarding broadcasts only to the necessary ports, preventing broadcast storms that can degrade network performance.
- **Spanning Tree Protocol (STP):** STP ensures loop-free topology in a network by identifying redundant paths and blocking them, preventing loops that could lead to broadcast storms.
- **Quality of Service (QoS):** Some advanced switches support QoS features, allowing prioritization of certain types of traffic to ensure a consistent and optimized network performance.

Technical Jargon – Switches – Types

- **Unmanaged Switch:** A basic plug-and-play switch with no configuration options. It operates seamlessly but lacks advanced features.
- **Managed Switch:** Offers control and configuration options, allowing network administrators to optimize performance, monitor traffic, and implement security measures.
- **PoE Switch (Power over Ethernet):** Provides power and data connectivity to devices like IP cameras and VoIP phones through a single Ethernet cable.
- **Stackable Switch:** Enables the connection of multiple switches to operate as a single unit, simplifying management and increasing scalability.

Technical Jargon – Routers

Routers are integral devices in computer networking that operate at the network layer (Layer 3) of the OSI model. They play a pivotal role in directing data packets between different networks, ensuring efficient and accurate data transmission.

Technical Jargon – Routers – Types

Traditional Routers:

- These are the basic routers used in home networks, providing connectivity between the local network and the Internet.
- Commonly used in residential and small business setups.

Enterprise Routers:

- Designed for larger networks, they offer advanced features like VPN support, enhanced security, and scalability.
- Suitable for organizations with complex networking requirements.

Core Routers:

- Situated at the core of large networks, they handle substantial data traffic.
- Used by Internet Service Providers (ISPs) to manage data flow across the internet.

Edge Routers:

- Located at the edge of a network, they connect local networks to external networks.
- Vital for managing communication between an organization's internal network and external entities.

Technical Jargon – Routers – Functionality

Routers operate based on the following key functionalities:

Path Determination:

- Routers use routing tables to determine the optimal path for data packets.
- Historical Dates: The concept of routing dates to the ARPANET era in the late 1960s.
- How Routing Works:

Packet Forwarding:

- Upon receiving a packet, routers examine the destination IP address and consult their routing table.
- The router then forwards the packet to the next hop on the determined path.

Path of Least Resistance:

Routers aim to choose the path of least resistance, optimizing data transmission. This involves considering factors like link speed, latency, and network congestion.

Technical Jargon – Routers – Routing Protocols

OSPF (Open Shortest Path First):

- An interior gateway protocol used within a single autonomous system.
- Introduced in RFC 2328 in 1998.

BGP (Border Gateway Protocol):

- An exterior gateway protocol used for routing between different autonomous systems.
- Initially defined in RFC 1267 in 1991.

EIGRP (Enhanced Interior Gateway Routing Protocol):

- Cisco's proprietary routing protocol offering advanced features.
- Initially documented in Cisco's publications, later standardizing in RFC 7868 in 2016.

Technical Jargon – DHCP

DHCP, or Dynamic Host Configuration Protocol, is a network protocol utilized to automate the assignment of IP addresses and other related network configuration parameters to devices in a network. This protocol operates on the application layer of the OSI model and plays a crucial role in simplifying network management.

Technical Jargon – DHCP – Purpose

The primary purpose of DHCP is to provide a dynamic and automated method for assigning IP addresses to devices within a network. This eliminates the need for manual IP configuration, making it efficient for both administrators and end-users. DHCP ensures that devices can seamlessly join and leave a network without requiring static IP assignments.

Technical Jargon – DHCP – Versions

1. **DHCPv1 (1985):** The concept of DHCP was introduced in 1985 as a proposed standard in RFC 903. This early version laid the groundwork for automated IP address assignment but lacked many features found in later iterations.
2. **DHCPv2 (1993):** The second version, documented in RFC 1541, improved upon the initial implementation, introducing support for multiple subnet configurations and enhancing overall reliability.
3. **DHCPv3 (1997):** The third version, specified in RFC 2131, further refined DHCP by adding mechanisms for network reconfiguration and dynamic DNS updates.
4. **DHCPv4 (2003):** Despite the commonly used term "DHCPv4," there isn't a distinct version labeled as such. Instead, improvements and clarifications were made through various RFCs, including RFC 2131 and RFC 3315.
5. **DHCPv6 (2007):** The introduction of IPv6 led to the development of DHCPv6, documented in RFC 3315, tailored for the unique characteristics of IPv6 addressing and configuration.

Technical Jargon – DHCP – Functionality

The DHCP process follows a structured sequence known as DORA:

Discover (D):

> The DHCP client broadcasts a DHCPDISCOVER message to discover available DHCP servers on the network.
>
> The message is typically sent over the broadcast address, and it contains essential client information.

Offer (O):

> DHCP servers receive the DHCPDISCOVER broadcast and respond with a DHCPOFFER message.
>
> This message contains a proposed IP address, subnet mask, lease duration, and other configuration parameters.
>
> The client can receive multiple offers but typically accepts the first one received.

Request (R):

> The DHCP client, having received one or more offers, sends a DHCPREQUEST message to the selected DHCP server.
>
> This message confirms the client's intent to use the offered configuration parameters.
>
> If multiple offers were received, this step identifies the chosen DHCP server.

Acknowledge (A):

> The selected DHCP server responds with a DHCPACK message, confirming the client's request.
>
> The DHCPACK message includes the final details of the accepted configuration, such as the assigned IP address and lease duration.
>
> The client now has a valid IP address and can proceed with network communication.

It's crucial to note that, in case of issues or conflicts during the DORA process, the DHCP server may respond with a DHCPNAK (Negative Acknowledgment) message, prompting the client to restart the process. If nothing happens I takes an IP from APIPA.

Understanding the DORA sequence illustrates how DHCP efficiently manages IP address assignment, configuration, and communication between clients and servers in a network. This process ensures a dynamic and streamlined approach to network connectivity without manual intervention.

Technical Jargon – DNS

DNS, or Domain Name System, is the backbone of the internet, translating user-friendly domain names into IP addresses that machines understand. This hierarchical system facilitates human interaction with computers, allowing us to access websites by names instead of complex numerical addresses.

The DNS journey commenced in the 1980s when Paul Mockapetris introduced it. Initially defined in RFC 882 and RFC 883 in 1983, DNS went through iterations, with RFC 1035 being the pivotal document that solidified its foundation.

Technical Jargon – DNS – Purpose

The primary purpose of DNS is to bridge the gap between human-readable domain names and IP addresses. It functions as a distributed database, ensuring efficient and quick translation of user queries into machine-understandable addresses.

Technical Jargon – DNS – Versions

DNS has evolved over time, with notable versions shaping its trajectory. Key versions include DNSv4, the most widely used, and the more recent DNSv6, designed to address the exhaustion of IPv4 addresses by introducing a larger address space.

Technical Jargon – Functionality

1. **Query Initiation:**
   User inputs a domain name (e.g., www.example.com), triggering the DNS resolution process.
2. **Root Server Interaction:**
   Resolver contacts a root DNS server, the initial point of contact, to obtain information about the top-level domain (TLD).
3. **TLD Server Inquiry:**
   Root server directs the resolver to the TLD server responsible for the specific domain extension (e.g., .com).
4. **Authoritative Server Engagement (First Round):**
   TLD server guides the resolver to the authoritative DNS server responsible for the top-level domain, initiating the quest for the domain's IP address.
5. **Authoritative Server Engagement (Second Round):**
   The authoritative server for the specific domain is queried, obtaining the actual IP address associated with the domain.
6. **IP Retrieval:**
   The authoritative server furnishes the resolved IP address to the resolver, completing the resolution process.
7. **Response to User:**
   The resolver provides the user's device with the obtained IP address, enabling it to establish a connection with the desired web server.

Technical Jargon – DNS Entry Types

CNAME (Canonical Name):

- **Function:** Allows aliasing one domain to another.
- **Example:** Alias www.example.com to example.com.

TXT (Text):

- **Function:** Stores text information, commonly used for verification or SPF records for email authentication.
- **Example:** Holds verification keys for domain ownership.

AAAA (IPv6 Address):

- **Function:** Resolves a domain to its IPv6 address, supporting the transition to IPv6.
- **Example:** Associates a domain with its IPv6 address.

A (IPv4 Address):

- **Function:** Associates a domain with its IPv4 address, the most common type of DNS record.
- **Example:** Links a domain like www.example.com to its IPv4 address.

NS (Name Server):

- **Function:** Specifies authoritative DNS servers for a domain.
- **Example:** Declares which servers are authoritative for a particular domain.

MX (Mail Exchange):

- **Function:** Identifies mail servers responsible for receiving emails on behalf of the domain.
- **Example:** Directs emails sent to user@example.com to the specified mail server.

PTR (Pointer):

- **Function:** Used for reverse DNS lookups, mapping an IP address to a domain name.
- **Example:** Resolves the domain associated with a given IP address.

Technical Jargon – Email

Email, short for electronic mail, is a method of exchanging digital messages over the internet. The concept of email can be traced back to the 1960s, with significant developments occurring over the years.

- **1960s:** The origins of email can be linked to MIT's Compatible Time-Sharing System (CTSS), where users could leave messages for each other.
- **1971:** Ray Tomlinson, a computer programmer, implemented the first system to send messages between users on the same computer.
- **1982:** The introduction of the Simple Mail Transfer Protocol (SMTP) standardized email communication over networks.
- **1983:** The Domain Name System (DNS) allowed the use of domain names in email addresses, marking a crucial step in email evolution.
- **1991:** The advent of the Multipurpose Internet Mail Extensions (MIME) standardized the format of email messages, enabling the inclusion of multimedia content.

Technical Jargon – Functionality

Email operates on a client-server model, involving various protocols and components.

- **User Agents (UA):** These are email clients or applications used by individuals to compose, send, receive, and manage emails.
- **Mail Transfer Agent (MTA):** Responsible for the routing and transfer of emails between servers. SMTP is a crucial protocol in this process.
- **Mail Delivery Agent (MDA):** Takes care of delivering emails to the recipient's mailbox.
- **Post Office Protocol (POP) and Internet Message Access Protocol (IMAP):** These are protocols that enable users to retrieve emails from a server. POP typically downloads messages to the local device, while IMAP allows users to access and manage emails directly on the server.

Protocols for Incoming and Outgoing:

- **Incoming:** IMAP and POP3 are commonly used protocols for receiving emails. IMAP keeps emails on the server, allowing for multiple devices to sync, while POP3 downloads them to the local device.
- **Outgoing:** SMTP (Simple Mail Transfer Protocol) is the standard for sending emails. It works collaboratively with IMAP or POP3 to ensure seamless communication between email clients and servers.