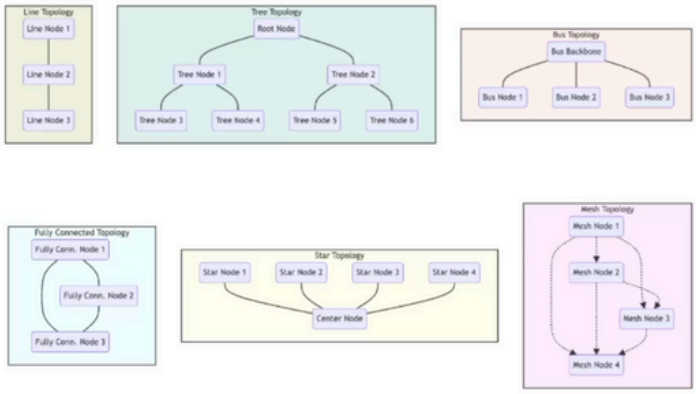
Topology and Addressing

- Understanding the network topology is crucial for security as it enables identification of potential vulnerabilities, optimal placement of security measures, and effective monitoring of network traffic flow.



Picture source: own creation

Topology and Addressing

- IP addressing is a crucial aspect of network communication, assigning unique numerical identifiers to devices for data routing. It is vital for security, enabling access control, firewall rules, and network segmentation to mitigate risks like unauthorized access and data breaches. Effective IP management aids in logging, monitoring network traffic, and detecting security threats, ensuring a secure network infrastructure.

Department	Device	IP Address
HR	Router	192.168.1.1
	Server	192.168.1.10
	Desktop PC 1	192.168.1.100
	Desktop PC 2	192.168.1.101
	Printer	192.168.1.50
IT	Router	192.168.2.1
	Server	192.168.2.10
	Desktop PC 1	192.168.2.100
	Desktop PC 2	192.168.2.101
	Printer	192.168.2.50
Finance	Router	192.168.3.1
	Server	192.168.3.10
	Desktop PC 1	192.168.3.100
	Desktop PC 2	192.168.3.101
	Printer	192.168.3.50

Picture source: own creation

Topology and Addressing

Subnetting

Prefix Length Slash Notation (CIDR)	Max Addresses (Total IPs)	Available Hosts (Usable IPs)	Subnet Length	Subnet Mask
/32	1	0	32	255.255.255.255
/31	2	0	31	255.255.255.254
/30	4	2	30	255.255.255.252
/29	8	6	29	255.255.255.248
/28	16	14	28	255.255.255.240
/27	32	30	27	255.255.255.224
/26	64	62	26	255.255.255.192
/25	128	126	25	255.255.255.128
/24	256	254	24	255.255.255.0
/23	512	510	23	255.255.254.0
/22	1024	1022	22	255.255.252.0
/21	2048	2046	21	255.255.248.0
/20	4096	4094	20	255.255.240.0
/19	8192	8190	19	255.255.224.0
/18	16384	16382	18	255.255.192.0
/17	32768	32766	17	255.255.128.0
/16	65536	65534	16	255.255.0.0
/15	131072	131070	15	255.254.0.0
/14	262144	262142	14	255.252.0.0
/13	524288	524286	13	255.248.0.0
/12	1048576	1048574	12	255.240.0.0
/11	2097152	2097150	11	255.224.0.0
/10	4194304	4194302	10	255.192.0.0
/9	8388608	8388606	9	255.128.0.0
/8	16777216	16777214	8	255.0.0.0
/7	33554432	33554430	7	254.0.0.0
/6	67108864	67108862	6	252.0.0.0
/5	134217728	134217726	5	248.0.0.0
/4	268435456	268435454	4	240.0.0.0
/3	536870912	536870910	3	224.0.0.0
/2	1073741824	1073741822	2	192.0.0.0
/1	2147483648	2147483646	1	128.0.0.0
/0	4294967296			

Picture source: own creation

Topology and Addressing

Special IPv4 Addresses

Name	Range	Subnet Mask
Local Host	127.0.0.0 – 127.255.255.255	Not applicable
APIPA	169.254.0.0 – 169.254.255.255	Not applicable

Bogon IPv4 Addresses

Name	Range	Subnet Mask
This network	0.0.0.0/8	Not applicable
Private IPv4 Block	10.0.0.0/8	Not applicable
Carrier-grade NAT	100.64.0.0/10	Not applicable
Loopback	127.0.0.0/8	Not applicable
Link local	169.254.0.0/16	Not applicable
IETF Assignments	192.0.0.0/24	Not applicable
Private IPv4 Block	172.16.0.0/12	Not applicable
TEST-NET-1	192.0.2.0/24	Not applicable
Benchmark testing	198.18.0.0/15	Not applicable
TEST-NET-2	198.51.100.0/24	Not applicable
TEST-NET-3	203.0.113.0/24	Not applicable
Multicast	224.0.0.0/4	Not applicable
Reserved	240.0.0.0/4	Not applicable
Limited broadcast	255.255.255.255/32	Not applicable

Class	Range	Subnet Mask
A	0.0.0.0 – 127.255.255.255.	255.0.0.0
B	128.0.0.0 – 191.255.255.255	255.255.0.0
C	192.0.0.0 – 223.255.255.255	255.255.255.0
D	224.0.0.0 – 239.255.255.255	Not applicable
E	240.0.0.0 – 255.255.255.255	Not applicable

Private IPv4 Addresses

Range	Subnet Mask
10.0.0.0 – 10.255.255.255	255.0.0.0
172.16.0.0 – 172.31.255.255	255.240.0.0
192.168.0.0 – 192.168.255.255	255.255.0.0.

Picture source: own creation

Topology and Addressing

- Static IP vs Dynamic IP (DHCP)

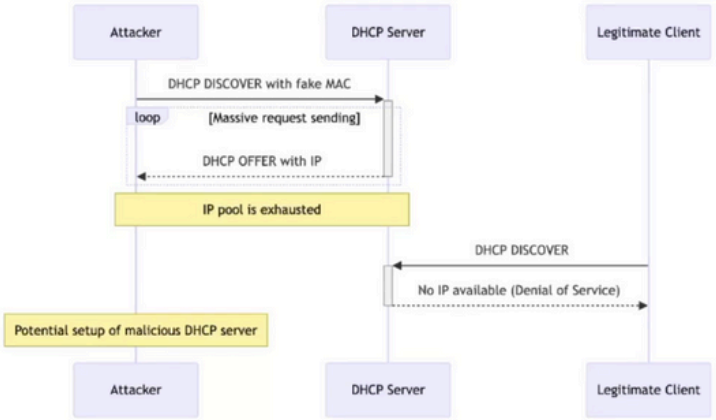
Aspect	Static IP Address	Dynamic IP Address
Security	Advantages	Disadvantages
- Network Access Control	Easier to implement access control lists.	Harder to manage due to changing IP addresses.
- Tracking and Monitoring	Simpler to track and monitor network activity.	More challenging due to the need to map IPs to devices constantly.
- Vulnerability to Attack	Potentially more vulnerable if not managed correctly as the IP is constant and can be targeted.	Less predictable, which can provide a layer of obscurity against targeted attacks.
- Configuration Complexity	Configuration is more complex and requires careful management.	Simplified configuration with DHCP.

Device Operation	Advantages	Disadvantages
- Network Stability	More stable network configuration as IPs do not change.	Potential for IP conflicts or exhaustion of IP pool.
- Remote Access	Easier for remote access and hosting services since the IP does not change.	More difficult to access remotely unless a Dynamic DNS service is used.
- Ease of Setup	Requires manual configuration which can be error-prone.	Automatic IP assignment simplifies setup for large numbers of devices.
- Device Identification	Permanent IP makes it easier to identify devices.	Dynamic assignment requires additional mechanisms to consistently identify devices.
- Scalability	Less scalable due to the manual assignmer ↓ Ps.	More scalable, especially in large networks with many devices.

Picture source: own creation

Topology and Addressing

- DHCP Security example: Starvation Attack (DoS)



Picture source: own creation

Topology and Addressing

- NAT, SNAT and DNAT

•**NAT**: A protocol that translates private IP addresses to a public IP address, allowing for internet connectivity and IP conservation.

•**SNAT**: Transforms the source IP address of outgoing traffic from a private network to appear as though it's originating from a different IP address.

•**DNAT**: Changes the destination IP address and port number of incoming traffic to route it to the appropriate host within a private network.