NETWORK 101 vol II

İSMET ARSLAN

$ whoami

- Cyber Security Researcher
- Co-founder & 2. president at KMU YBT
- Karaman Province Represntative at Altair Cyber Club
- Karamanoglu Mehmetbey University Computer Engineering

https://tr.linkedin.com/in/ismet-arslan-31050914a

@4rslanismet

Site: cyberv4gus1337.wordpress.com

Mail: arslanismet@protonmail.com

$ ls

-> TCP / IP Yapısı

-> TCP / IP İletişimi İçin Gerekli Parametreler

->ARP

-> ICMP

-> IP

-IP Adresleme

-> TCP

-> UDP

- > Sık Kullanılan Portlar

- > NAT (Network Adress Translation) Nedir ?

-> Subnetmask & Subnetting Nedir ?

-> IPv6

-> HTTP

-> HTTPS

-> FTP

-> SSH

-> SNMP

-> DNS

-> Sorular

TCP / IP

- TCP/IP yani biraz açarsak “Transmission Control Protocol / Internet Protocol” internet üzerinde iletişimi sağlayan protokoller kümesidir. TCP/IP bir çok protokolü içerisinde barındırmaktadır. Sahip olduğu kurallar çerçevesinde ağlara dahil olan cihazları birbiri ile iletişim kurabilir kılmaktadır.

TCP / IP

- TCP/IP protokolü içerisinde cihazların birbirileri ile iletişime geçebilmesi için bazı parametrelere gerek duyulmaktadır. Bunları şöyle listeleyebiliriz.
- -Hostname (Bilgisayar Adı)
- -IP Adresi
- -MAC Adresi

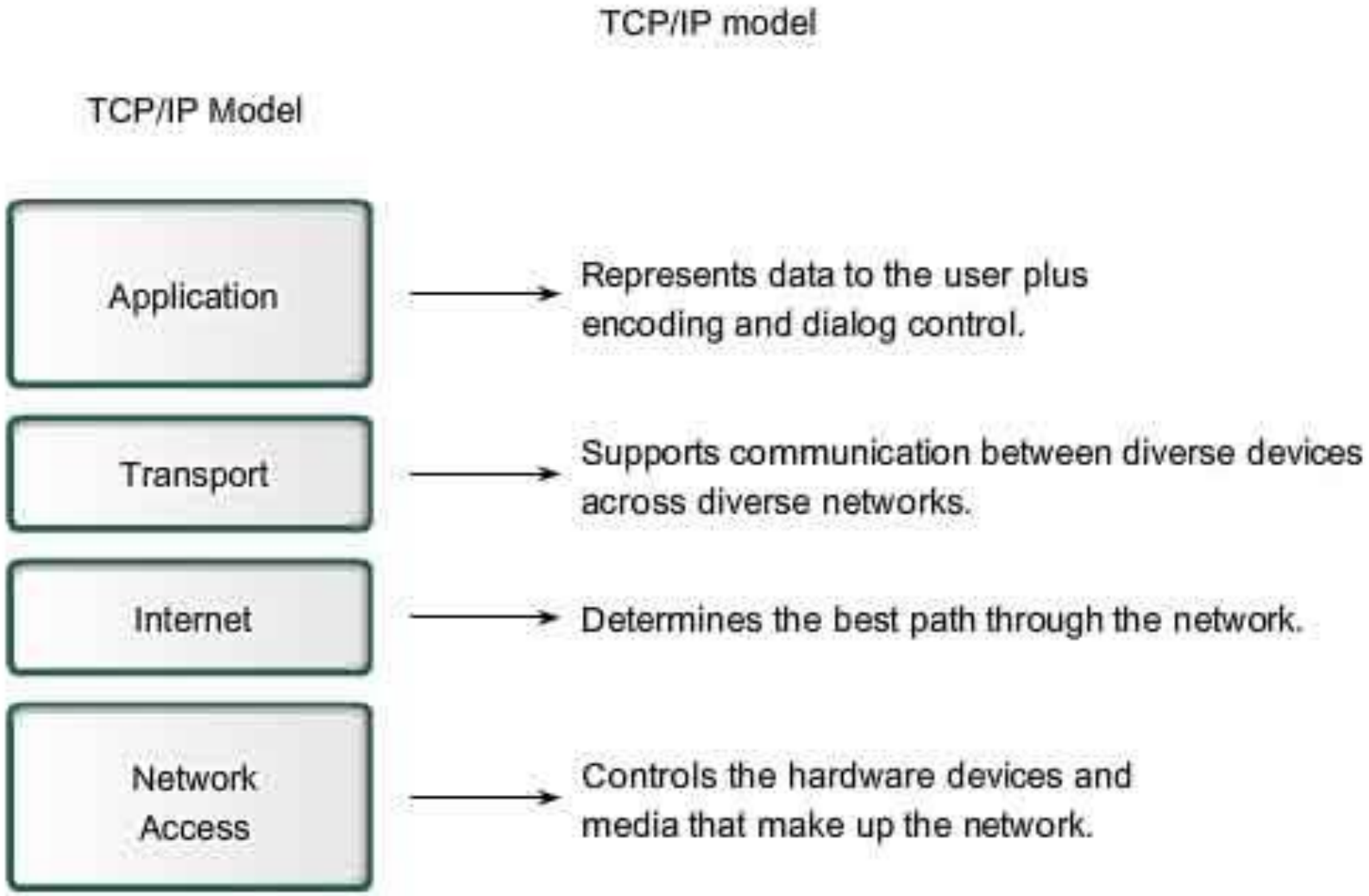
TCP / IP

- Biraz açalım;
- -Hostname nedir?
- Hostname, sistemlerin aldığı isimdir. Kullanıcılar tarafından sistemi tanımlamak amacıyla atanır.
- -IP Adresi nedir?
- IP adresi TCP/IP protokolü üzerinden iletişim kuran cihazların birbiriyle ilişimde kullandıkları adrestir.
- -MAC Adresi nedir?
- Ağ kartlarının sahip olduğu benzersiz adrestir. Fiziksel adres ibareside kullanılır. 6 oktetten oluşur ve 48 bitlik bir adrestir.

TCP / IP

- **MAC Adresini biraz daha açalım..**
- **Dediğimiz gibi 6 oktetten oluşan bir yapıya sahiptir.**
- **Örn: 01:23:45:67:89:AB**
- **Oktetler birbirilerinden ":" ile ayrılmaktadır ve herbiri 8 bittir.. İlk 3 oktet üretici firmaya aittir. Sonraki 3 oktet ise üretici firma tarından karta verilen ve benzersiz niteliği taşımasını sağlayan kısımdır.**
- **Yerel ağlardaki haberleşme için kullanılmaktadır. Farklı ağlarda bulunan cihazların iletişimini sağlamak için yetersizdir**

TCP / IP Yapısı



- **4 katmandan oluşmaktadır. Bu katmanları yadaki görselle tanıyabiliriz.**

ARP – Adress Resolution Protocol nedir?

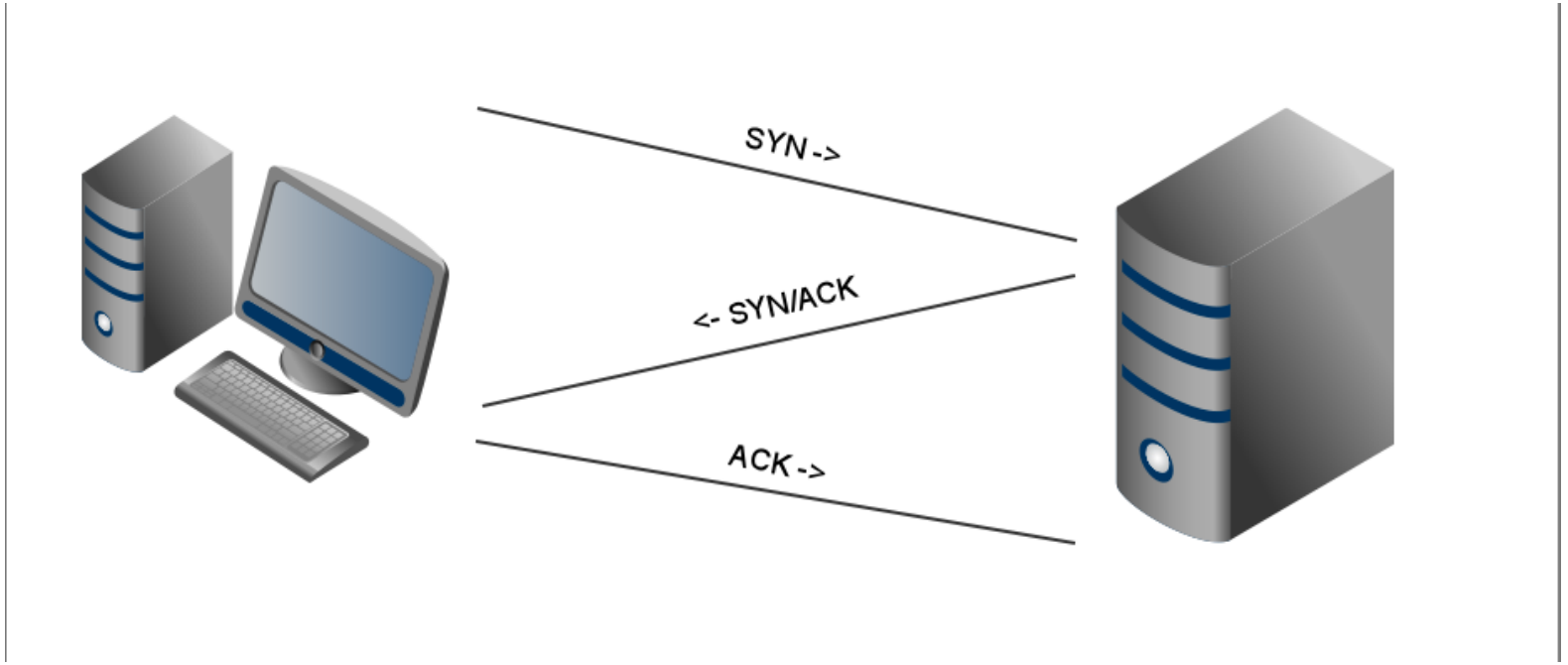
- TCP/IP de iletişim için kullanılan 32 bitlik IP adresini ağ kartlarına tanımlanan benzersiz (48 bitlik) MAC adreslerine çevirme işlemini yapar. ARP tablosu ile iletişimde olunan sistemlerin IP adresleri ve MAC adresleri tanımlanır ve öğrenilir.
- Bir cihaz iletişime geçeceği diğer cihazın IP adresinde ARP Request göndererek MAC adresinin iletilmesini talep eder. ARP Reply paketi ile gelen karşılıklı olarak iletişim tamamlanır ve MAC adresleri ARP tablolarına yerleştirilir.

ICMP – Internet Control Message Protocol nedir?

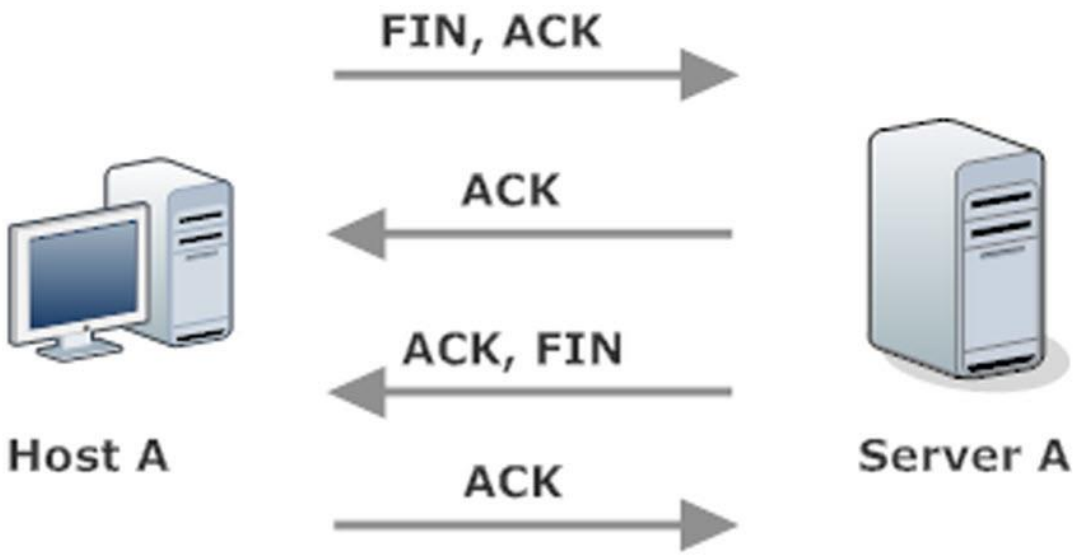
- Kontrol amaçlı oluşturulmuş/kullanılan bir protokoldür. Sistemler arası iletişimin test edilmesi amacıyla sıkça kullanılmaktadır. Ping komutu ICMP protokolü ile iletişim kurduğu bilgisayara erişimi kontrol etmektedir.

TCP – Transmission Control Protocol Nedir?

- Güvenilir, kayıpsız ve kontrol edilebilir iletişimi sağlamak amacıyla kullanılmaktadır. İletişimde olan iki bilgisayarın kontrolü çerçevesinde ilerleyen bir bağlantı söz konusudur. Verilerin gönderilmesi öncesi cihazlar birbirilerinde 3-Way Handshake yöntemiyle oturum açarlar.



3-Way Handshake Nedir ?



4-way Handshake Nedir ?

IP Adresleme

- **IPv4 Hakkında;**
- **IPv4 günümüzde en yaygın kullanılan adresleme protokolüdür.**
- **32 bittir ve 2 üzeri 32 yani 4,294,967,196 adet ip adresi ile adresleme yapmaktadır.**
- **4 oktetten oluşmaktadır ve oktetler 0-255 arası değer almaktadır.**

UDP – User Datagram Protocol Nedir?

- TCP nin aksine güvensiz, kontrolsüz ve bağlantı gerektirmeyen bir protokoldür.
- Gönderilen verinin nereye gittiği, nasıl gittiği, gitti mi gitmedi mi derdi yoktur.
- DNS 53 , TFTP, SNMP gibi protokollerde kullanılır.

Port Nedir ?

- **Sistemlerde çalışan bir çok servis ve uygulama ve iletişimde bulunulan bir çok farklı cihaz var ve bunların iletişimi için kullanılan adı Port olan sanal kapılar var.**
- **Port numaraları 0-65535 arasında herhangi bir değer alabilir. İlk bin port iyi bilinen portlar arasında yer almaktadır ve en çok kullanılan servis ve yazılımların kullandığı portlardır.**

Port Number	Protocol	Application
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP,TCP	DNS
67,68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL
16,384-32,767	UDP	RTP-based Voice and Video

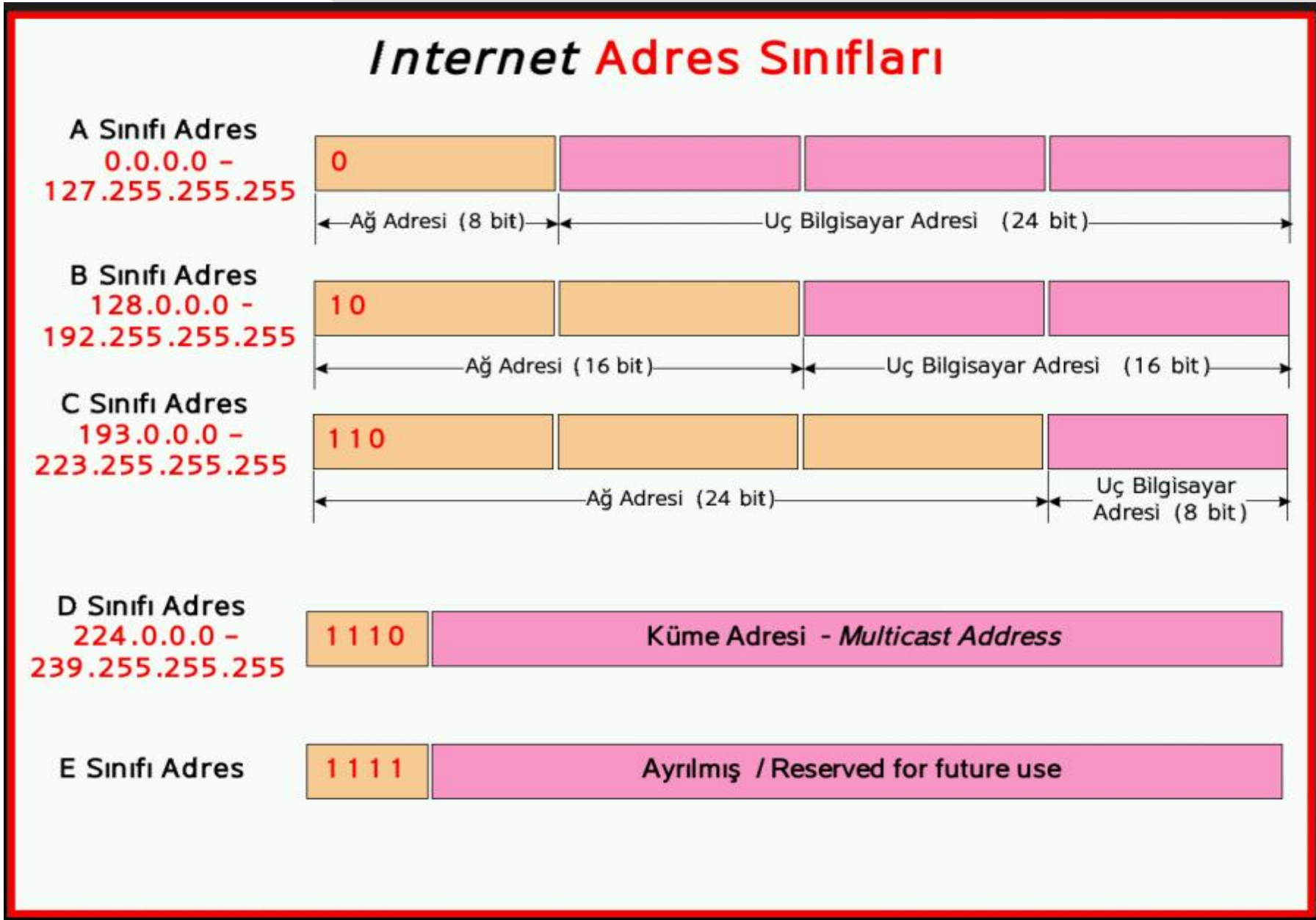
Sık Kullanılan Portlar

IP Adresleme

- **IP Adresi sistemlerin iletişimi için kullanılan bir adrestir. Şuan yaygın olarak IPv4 kullanılmaktadır ve yavaştan IPv6'ya doğru geçiş yapılmaktadır.**
- **Bu sunumda her ikisi hakkında kısa ve öz bilgiler yer almaktadır.**

IP Adresleme

IPv4 Sınıfları;



IP Adresleme

- **IPv4 Özel IP Aralıkları;**

- **Loopback IP (127.x.x.x) : Sistemin kendisine ait IP adresidir ve kendisini işaret eder.**
- **Apipa IP (169.254.0.0/16) : Sistemin IP alamaması durumunda kendine atadığı adrestir.**
- **Local IP Aralıkları : Yerel ağlara tanımlanan IP adresleridir.**
- **10.0.0.0 – 10.255.255.255**
- **172.16.0.0 – 172.31.255.255**
- **192.168.0.0 – 192.168.255.255**

NAT (Network Adress Translation) Nedir ?

- **Localdeki bir sistem aldığı Local IP ile internete çıkamamaktadır. Yönlendirici sayesinde, Reel bir IP adresi ile haritalama işlemi yaparak internete çıkabilir. Bu işleme NAT denmektedir.**

Subnet Mask & Subnetting Nedir ?

Subnet mask quick reference							
Host Bit length	math	Max hosts	Subnet mask	Mask octet	Binary mask	Mask length	Subnet length
0	2^0=	1	255.255.255.255	4	11111111	32	0
1	2^1=	2	255.255.255.254	4	11111110	31	1
2	2^2=	4	255.255.255.252	4	11111100	30	2
3	2^3=	8	255.255.255.248	4	11111000	29	3
4	2^4=	16	255.255.255.240	4	11110000	28	4
5	2^5=	32	255.255.255.224	4	11100000	27	5
6	2^6=	64	255.255.255.192	4	11000000	26	6
7	2^7=	128	255.255.255.128	4	10000000	25	7
8	2^8=	256	255.255.255.0	3	11111111	24	8
9	2^9=	512	255.255.254.0	3	11111110	23	9
10	2^10=	1024	255.255.252.0	3	11111100	22	10
11	2^11=	2048	255.255.248.0	3	11111000	21	11
12	2^12=	4096	255.255.240.0	3	11110000	20	12
13	2^13=	8192	255.255.224.0	3	11100000	19	13
14	2^14=	16384	255.255.192.0	3	11000000	18	14
15	2^15=	32768	255.255.128.0	3	10000000	17	15
16	2^16=	65536	255.255.0.0	2	11111111	16	16
17	2^17=	131072	255.254.0.0	2	11111110	15	17
18	2^18=	262144	255.252.0.0	2	11111100	14	18
19	2^19=	524288	255.248.0.0	2	11111000	13	19
20	2^20=	1048576	255.240.0.0	2	11110000	12	20
21	2^21=	2097152	255.224.0.0	2	11100000	11	21
22	2^22=	4194304	255.192.0.0	2	11000000	10	22
23	2^23=	8388608	255.128.0.0	2	10000000	9	23
24	2^24=	16777216	255.0.0.0	1	11111111	8	24

IPv6

- IPv6 günümüzde yeni yaygınlaşan ve IPv4'ün yetersiz kalması ile ortaya çıkmış adresleme protokolüdür.
- 128 bittir ve 2 üzeri 128 adet ip adresi ile adresleme yapmaktadır.
- 8 oktetten oluşmaktadır ve oktetler 16 bitliktir.

HTTP (Hyper Text TransferProtocol)

- **HTTP** (İngilizce *Hyper-Text Transfer Protocol*, Türkçe *Hiper Metin Transfer Protokolü*) bir kaynaktan dağıtılan ve ortak kullanıma açık olan hiperortam bilgi sistemleri için uygulama seviyesinde bir iletişim kuralıdır.

HTTPS (Secure Hyper Text Transfer Protocol)

- **HTTPS** (İngilizce *Secure Hypertext Transfer Protocol*, Türkçe **güvenli hiper metin aktarım iletişim kuralı**) hiper metin aktarım iletişim kuralının (HTTP) güvenli ağ protokolü ile birleştirilmiş olanıdır. Klasik HTTP protokolüne SSL protokolünün eklenmesi ile elde edilir.

FTP (File Transfer Protocol)

- **Dosya aktarım iletişim kuralı**, (İngilizce: **F**ile **T**ransfer **P**rotocol; **FTP**), bir veri yığınının - ASCII, EBCDIC, ve binary- bir uç aygıttan diğerine iletimi için kullanılmaktadır.

SSH (Secure Shell Protocol)

- **SSH** (Secure Shell) güvenli veri iletimi için kriptografik ağ protokolüdür. Ssh ile ağa bağlı olan iki bilgisayar arasında veri aktarımı güvenlik kanalı üzerinden güvensiz bir ağda yapılır. Bu durumda ağda Ssh ile haberleşen makinelerden biri ssh sunucusu diğeri ssh istemcisi olur. Bu protokol şartları SSH-1 ve SSH-2 olmak üzere iki önemli sürüm üzerinden birbirinden ayrılır.

SNMP (Simple Network Management Protocol)

- **Basit Ağ Yönetim Protokolü**, (İngilizce: **Simple Network Management Protocol**) bilgisayar ağları büyüdükçe bu ağlar üzerindeki birimleri denetlemek amacıyla tasarlanmıştır.

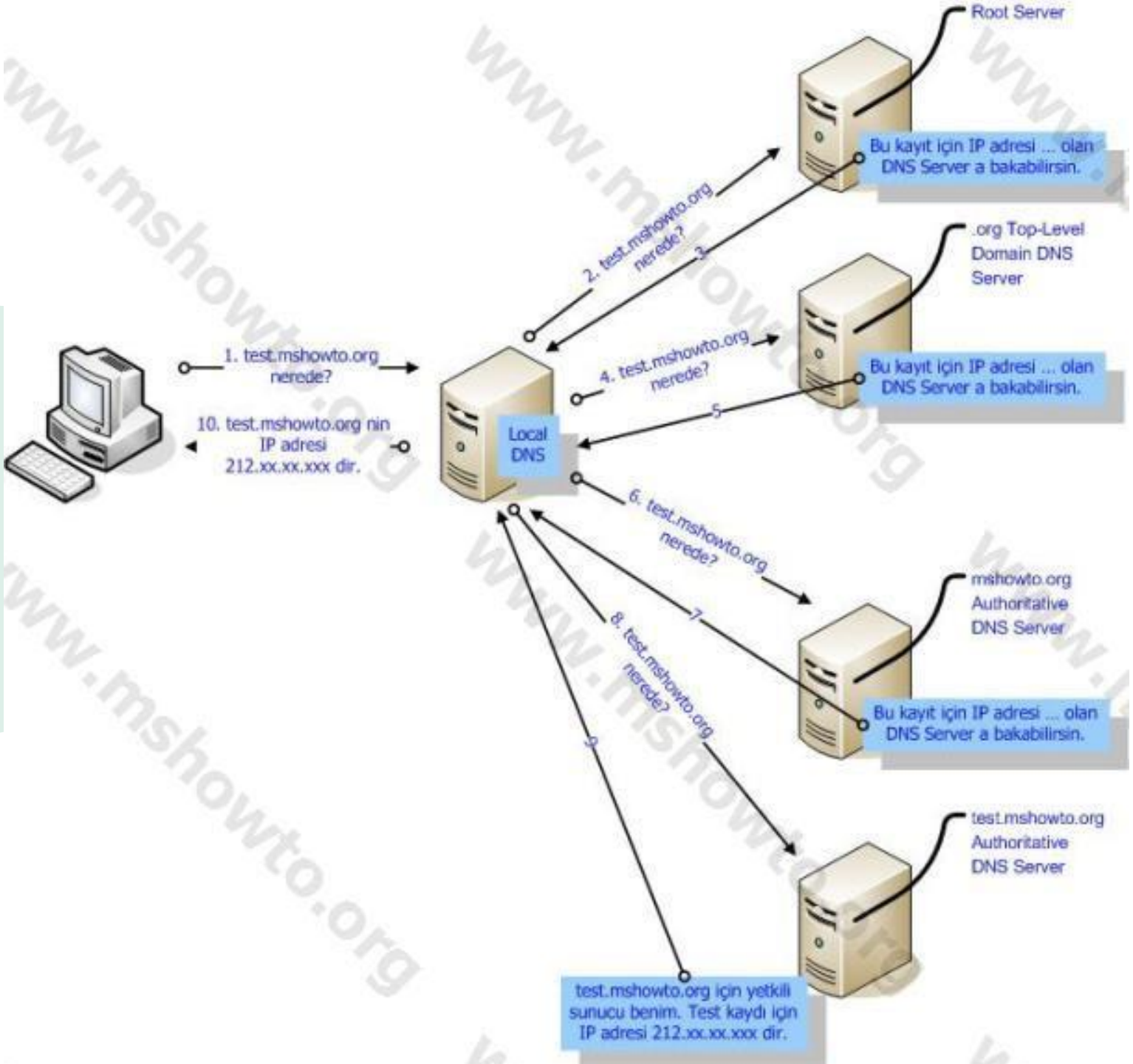
SMTP (Simple Mail Transfer Protocol)

- Elektronik posta **gönderme protokolü** (**S**imple **M**ail **T**ransfer **P**rotocol), bir e-posta göndermek için sunucu ile istemci arasındaki iletişim şeklini belirleyen protokoldür.

DNS (Domain Name System)

- **DNS** (İngilizce: ***D****omain* ***N****ame* ***S****ystem*, Türkçe: **Alan Adı Sistemi**), internet uzayını bölümlemeye, bölümleri adlandırmaya ve bölümler arası iletişimi organize etmeye yarayan bir sistemdir.

DNS Nasıl Çalışır ?



Questions

Teşekkürler