Eski den ip dağıltıımı -> arpanet

Iana -> ip adreslerinin protokolleri, iplerin dağıtımı

Icann ->

Router : anahtarlamaaya yarıyor.

Access point -wirles controllera bağlı olmalı. Tavanda yanan ışıklı kutudur

Firewal: neyin geçip geçemeyeceğini belirtir.

Ağa bağlannan router : virtual router

Accesspoint : 4 tane anteni, var içinde ve farklı frekanslarda haber veriyor. Cihazlar bağlanıyor.

Cicso lan contol: Access pointleri tek bir noktadan yöneten kontrol noktası

Adsl, landan wana geçerken kullanılır. Routing yapar.

Bridge(köprülerin ) yerine rouderlar,

Hubların yenie switchler aldı.

Bridge ve hublar çok kullanılmıyor..

Vpn, güvenli bir ağ oluşturur. Wan ile lan arasında. Trafiği şifreliyor ve güvenlik sağlyo

Ipv4 adresi, cihazın identifyıdır.

Subnetmask: vatandaşlığın hangi ülkeye ait olduğu

Ipconfig:

Icmp

Default gatewaye: paket gönderrirken buraya gider. Buraya ping atarak gateway var mı yokmu diye öğrenebiliriz.

Ttl : time to liave : kaç adımda geçtiği anlamına gelir.

1960larda hawaideki biri

Trace komutu:

Windows: tracert [www.google.com](http://www.google.com) //giderkenki gittiği yolları verir

Ping .com -t

Round trip timeı gösterir.: kaynaktan çıkıp hedee varırken ortalama, en iyi, en kötü ulaşma süresini verir

Traceroute ip\_ad

Apipa protokolü: her 5 saniyede bir tcp bağlantısı varm I diye bakar windows içinde

Windowsto “ ipadresi – “ yapınca o ip ile yapabileceğimiz confları verir.

Cpt de örnek “log ?”

ICMP: bu scotunu aldığım paketleriniletilmesini sağlar

Logical topologies:

Bus topology:

Maliyeti daha ucuzdur. Timeline

Description automatically generated

Tek bir bağ kopsa bile tüm sistem etkilenir.

Chart

Description automatically generated

Kullanıcılar merkezi bir cihaz üzerinden haberleşir. Arıza daha az gerçekleşir

Dezavantaj: merkezi kaybedersen patlar. Yedeklemek gerekir bu durumda

Diagram

Description automatically generated, fullmash: best practice

Dezavantaj: maliyet, her cihaza 5 tane kablo çerkersin.

Mühendislikte çalışan birinin finansta çalışan elemanların bilgilerine erişmesi istenmeyen bir durumdur.

Firewall bunu engeller

Vlanlarda da güvenlik önlemi alınabiliyor ama yeterli değil (Sanal güveenlik mi sağlıyor)

Unicast: bir noktadan bir noktaya

Broadcast haberleşme için (hepsine)255.255.255.255 e yayın yaparız

Herkese duyuruyoruz. Subnet maska göre cihazların o ağda olduğuuna karar veriliyordu (heralde)

Multicast: bir gruba yayın yapıyoruz. O gruba aitse cevap veriyor.

Hub: aptal bir cihaz.

Colision: birden fazla cihazın aynı anda paylaşılan ortamda veri iletmesiyle paketler çarpışır.bir algoya göre sıraya konur

Osi modeli abd tarafından geliştirilmiştir fakat sonra tcpip modeli avrupalılar tarafından geliştirileriek tüm dünyaca kabul edilmiştir. Cihazlarda bu model vardır

Diagram

Description automatically generated

Timeline

Description automatically generated