AĞ PROTOKOLLERİ

Mustafa NUMANOĞLU

İçerik

1. 802.1x Hakkında Genel Bilgi
2. ARP (Adres Çözümleme Protokolü)
3. BGP (Border Gateway Protocol - Sınır Geçit Protokolü)
4. CDP (Cisco Discovery Protocol - Cisco Tanımlama Protokolü)
5. DTP (Dynamic Trunking Protocol-Dinamik Gövdem Protokolü)
6. GLBP (Ağ Geçidi Yük Dengeleme Protokolü)
7. HTTP & HTTPS
8. ICMP (Internet Control Message Protocol-İnternet Kontrol Mesaj Protokolü)

İçerik

9. MPLS (Multi Protocol Label Switching - Çoklu Protokol Etiket Anahtarlama)
10. Point to Point Protocol (Noktadan Noktaya Protokolü)
11. PPP (Point to Point Protocol - Noktalar Arası İletişim Kuralı) Kimlik Doğrulama Metodları
12. SIP (Session Initiation Protocol - Oturum Başlatma Protokolü)
13. Spanning Tree Protokol
14. VTP (VLAN Trunking Protocol - Sanal Yerel Ağ Aktarım Protokolü)
15. Yönlendirme (Routing) Protokolleri

Protokol Nedir?

- Protokol, iki bilgisayar arasındaki iletişimi sağlamak amacıyla verileri düzenlemeye yarayan, standart olarak kabul edilmiş kurallar dizisidir.
- İki sistem arasında iletişim için kullanılan dili, yani mesajlaşma kurallarını belirtir. "Dil" yerine "protokol" kelimesinin seçilmiş olmasının sebebi, bu kelimenin programlama dili terimi tarafından önceden kullanılıyor olmasından kaynaklanır.

Ağ Protokollerinin Yapısı

- Sistemler iletişim için tek bir protokol kullanmazlar. Bunu yerine, protokol ailesi yada diğer bir deyişle protokol takımı kullanırlar. Protokollerin birbirleriyle iletişiminin koordinasyonu için konsept bir yapı gereklidir. Bunu sağlayacak yazılım hem protokolü, hem de 'xfer-mekanizmasını' sağlamak zorundadır.
- Xfer-mekanizması aracılığıyla iletişim sağlanır. Bu mekanizma sistem protokolleri ve diğer protokollerle olan iletişimler için bağımsız bir çalışma çevresi tanımlar. Protokoller bilgisayar iletişimi için kullanılırken programlama ise işlem için kullanılır.

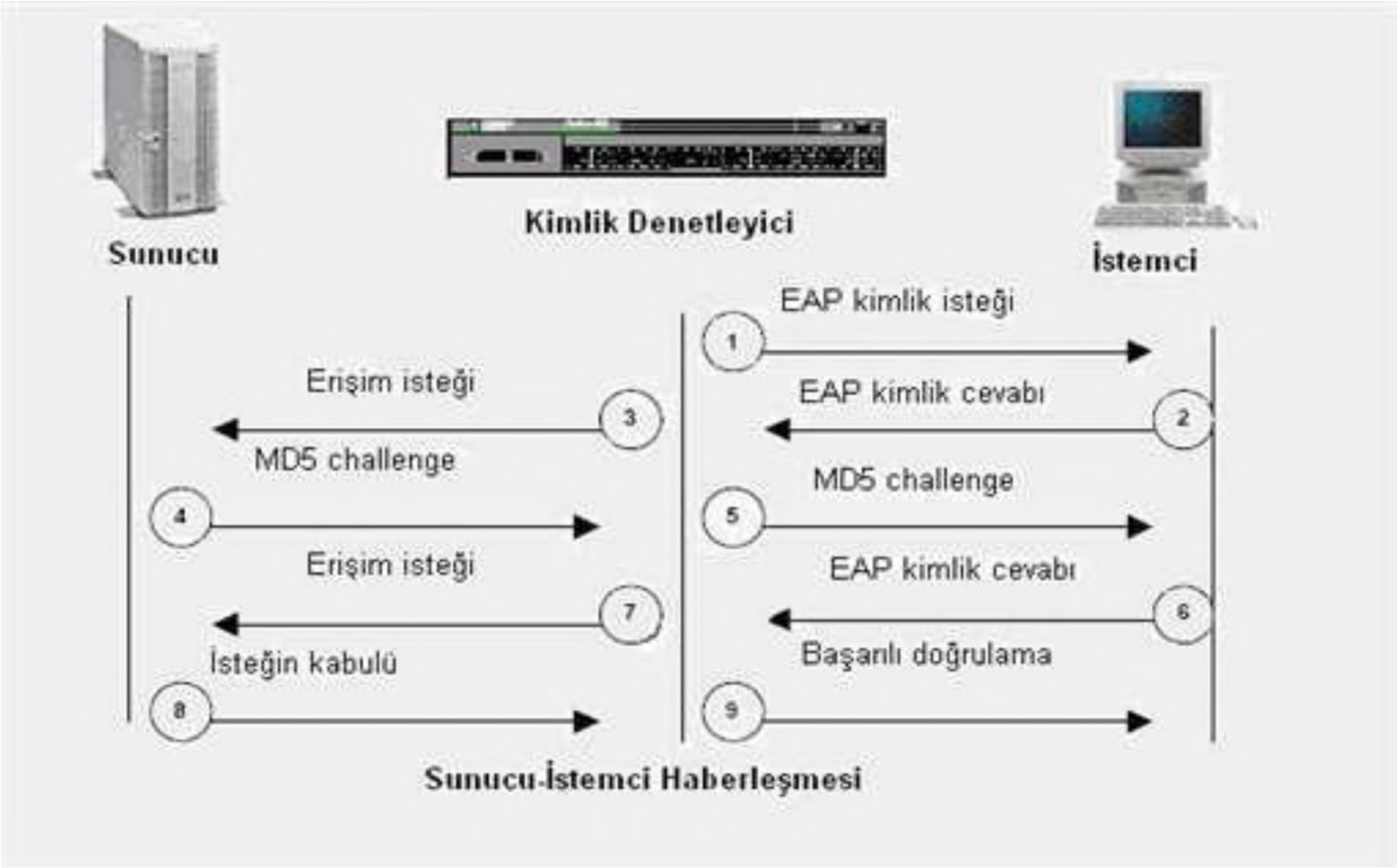
Ağ Protokollerinde Güvenlik

- 802.1x' in hedefi, yerel ağ (LAN) ve kablosuz yerel ağda (WLAN) standart bir güvenli kimlik denetimi (authentication) sağlamaktır. IEEE 802.1x en az sayıda yönetici ek yüküyle çok daha geniş alanlara güvenli bir şekilde ulaşmayı sağlar.
- Kullanıcılar kimlik denetimi işleminden sonra ağa erişebilirler, kimlikleri onaylanmayanlar ise erişemezler. Genelde bu tür kimlik doğrulama işlemleri e-posta, intranet (iç ağ) ve diğer özel uygulamalarda kullanılır. 802.1x'de 3 ana eleman kullanılmaktadır.
  - **İstemci**
  - **Kimlik denetleme sunucusu (authentication server)**
  - **Kimlik denetleyici (authenticator)**

Ağ Protokollerinde Güvenlik

- **İstemci:** Kimliğinin denetlenmesini isteyen taraftır.
- **Kimlik Denetleme Sunucusu (Authentication Server):** Kimlik denetleme işlemini gerçekleştiren asıl sunucudur.
- **Kimlik Denetleyici (Authenticator):** İstemciyle kimlik denetleme sunucusunun arasında bulunur. Ethernet anahtarlayıcı (ethernet switch) ya da kablosuz erişim noktası (wireless access point) birer kimlik denetleyicidir.

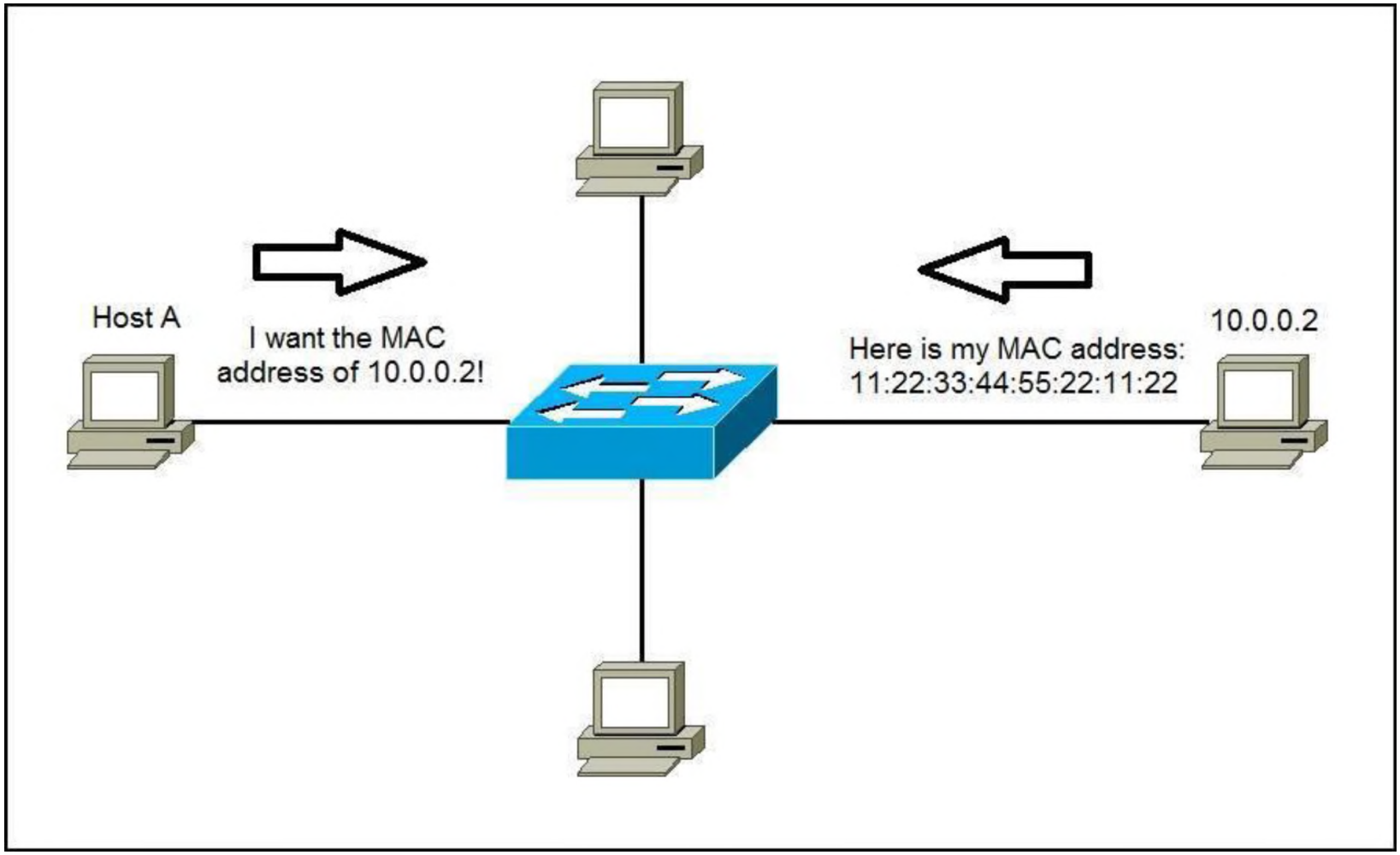
Sunucu - İstemci Haberleşmesinde Güvenlik



1. ARP (Adres Çözümleme Protokolü)

- Yerel ağlarda kullanılan en yaygın arayüz Ethernet'tir. Ethernet arayüzüne sahip olan ağ kartları ile yerel ağlara kolayca bağlanılmaktadır. Bu arayüzler birbirlerine paket göndermek için kendilerine üretim aşamasında verilmiş 48 bitlik fiziksel adresleri (mac adresi) kullanırlar. TCP/IP protokolü ise veri gönderip almak için 32 bit'lik IP adreslerini kullanır.
- Yerel ağda haberleşmek için veri alış-verişi yapılacak cihazın fiziksel adresi bilinmelidir. Bu işlem için kullanılan protokole, yani IP'si bilinen cihazın fiziksel adresinin öğrenilmesi protokolüne **Adres Çözümleme Protokolü** (Address Resolution Protocol) denir.

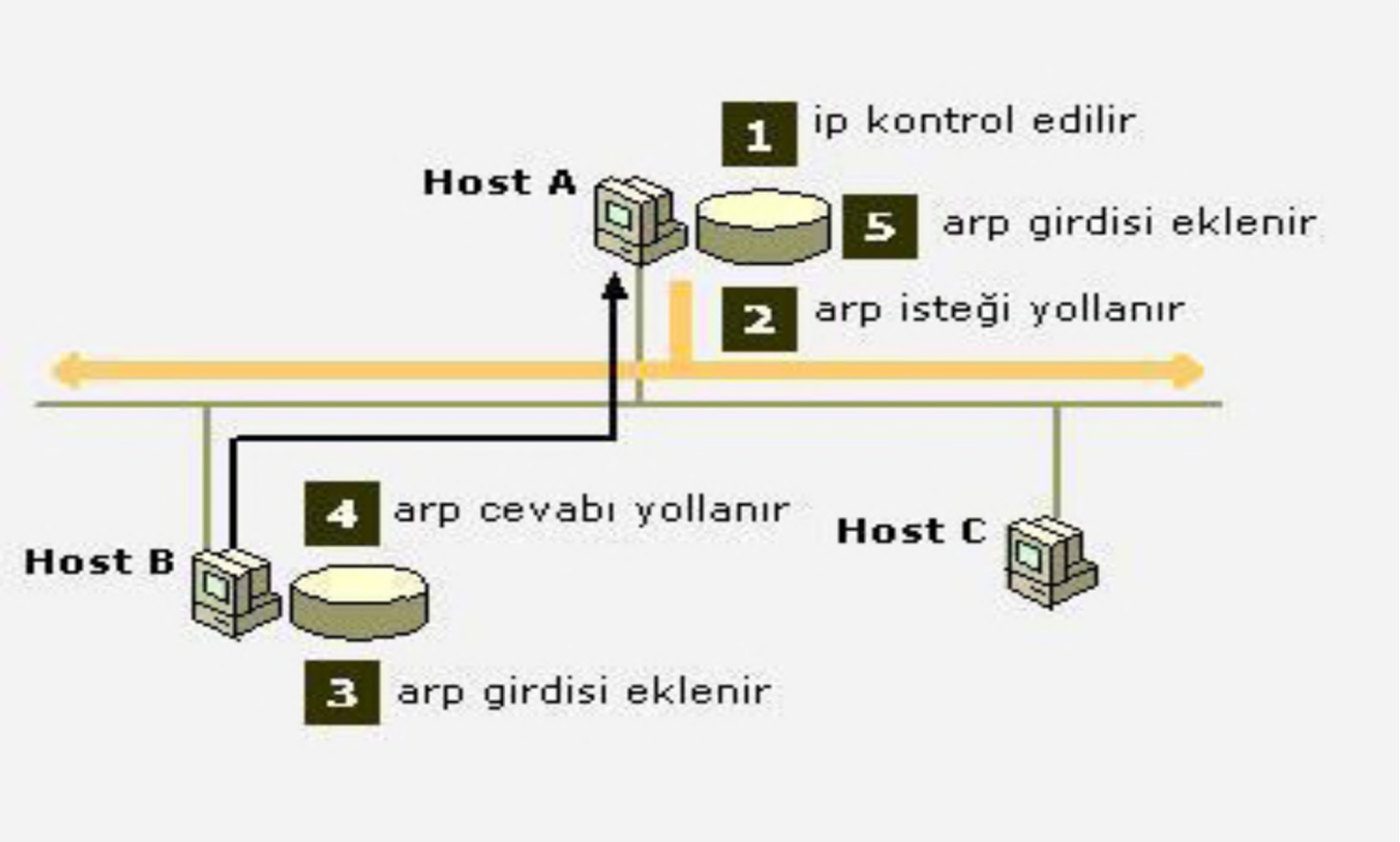
Address Resolution Protocol



Arp İsteği Paketi

- IP'si bilinen fakat fiziksel adresi bilinmeyen bir cihaz varsa bütün ağa **arp isteği (arp request)** gönderilir. Bu pakette gönderenin IP adresi, gönderenin fiziksel adresi ve alıcının IP adresi vardır. Alıcının fiziksel adresi bilinmediğinden tüm ağa yayın yapan (broadcast) bir paket yollanır ve isteğin bütün ağa ulaşması sağlanır.
- Belirtilen IP'nin dışındaki hiçbir IP'den cevap gelmez ve gelen cevap cihazın kendi fiziksel adresini içerir. Ayrıca isteği yollayan ve isteği yanıtlayan 2 cihazda diğerinin fiziksel adresini ve IP adresini daha sonra kullanmak üzere belleğine kaydeder.

Arp İsteği Paketi



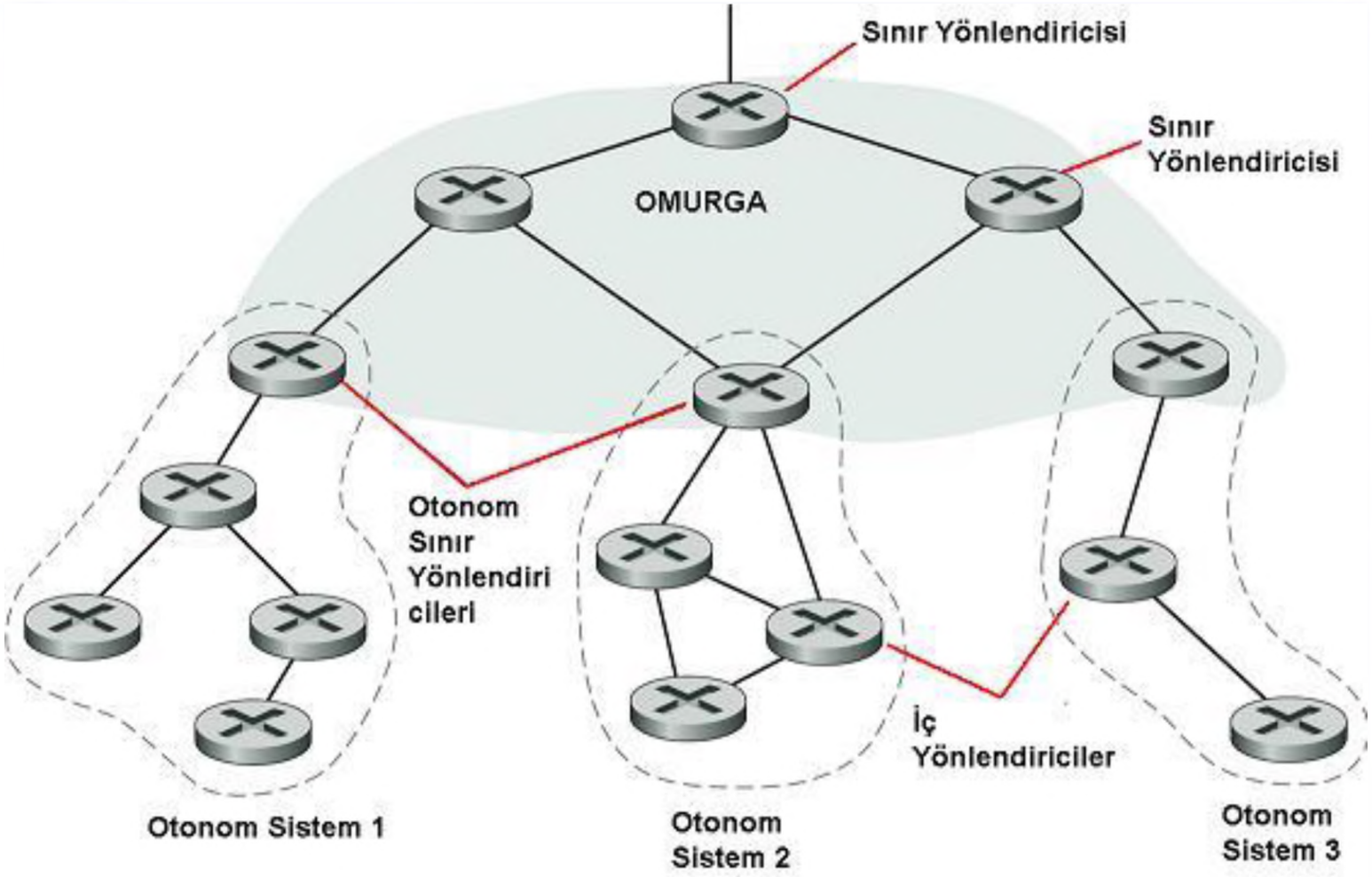
2. BGP (Border Gateway Protocol - Sınır Geçiş Protokolü)

- Routing protokolleri IGP (Dahili Ağ Geçidi Protokolü - Interior Gateway Protocol) ve EGP (Harici Ağ Geçidi Protokolü - Exterior Gateway Protocol) olmak üzere temelde ikiye ayrılırlar. Adından da anlaşılabileceği gibi IGP, iç networkte yani aynı AS (Otonom Sistem - Autonomous System) içerisinde kullanılan routing protokollerine verilen addır. EGP ise networkler arası, başka bir deyişle AS'ler arası kullanılan protokollerin geneline verilen bir isimdir. BGP (Border Gateway Protocol) de bir EGP'dir.
- BPG taşıma protokolü olarak TCP'yi kullanır. TCP güvenilir olduğu için hata düzeltme ya da yeniden iletim gibi mekanizmaları barındırmaz. Komşu olarak konfigüre edilen cihazlarla bir TCP haberleşmesi kurar ve bu bağlantıyı sürekli açık tutar.

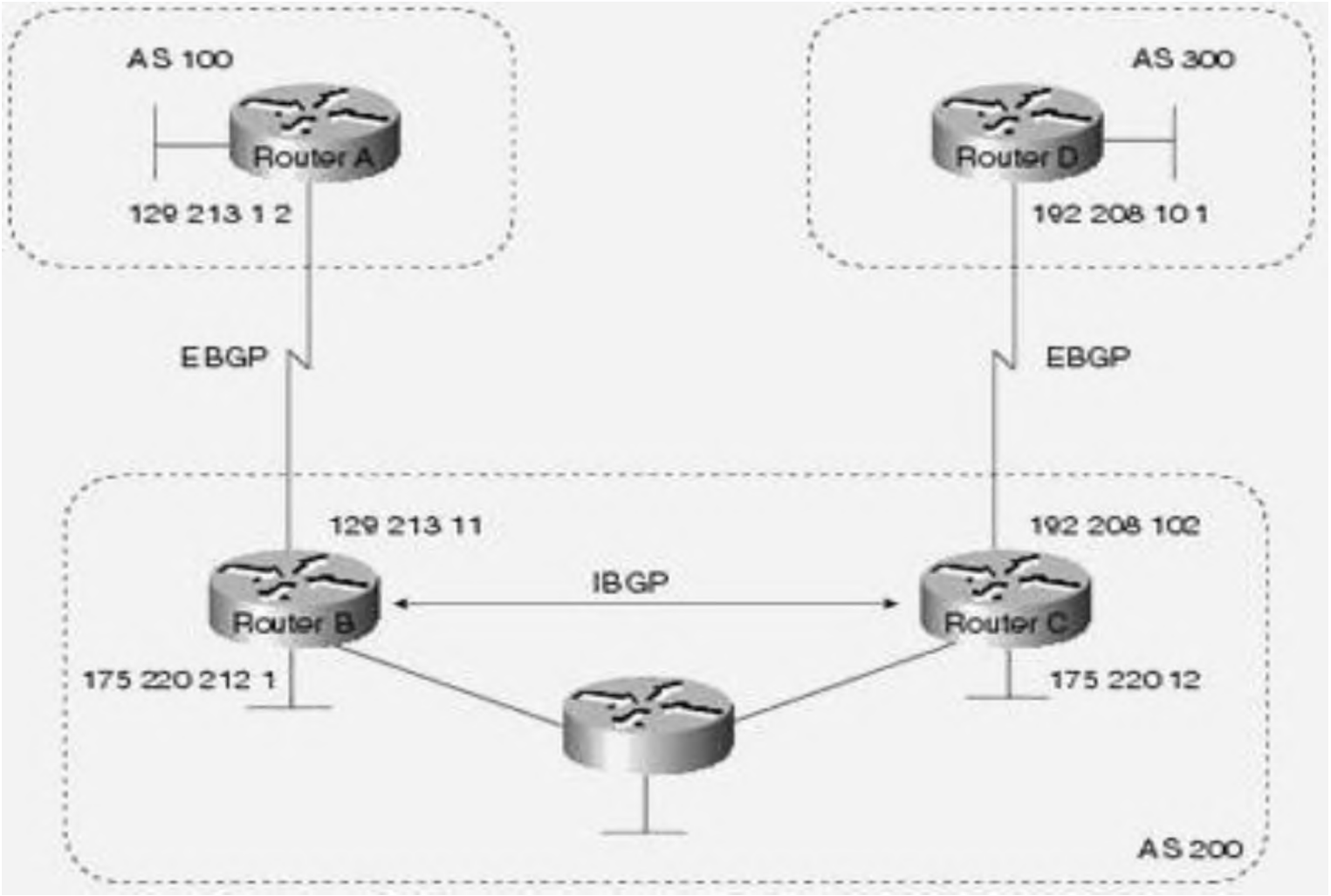
2. BGP (Border Gateway Protocol - Sınır Geçiş Protokolü)

- BGP çalıştıran bir router 3 farklı tablo tutar. Bunlardan ilki routera direkt olarak bağlı olan routerların tablosunun tutulduğu komşuluk tablosu (Neighbor Table), ikincisi bu komşulardan alınan tüm networklerin bilgilerinin tutulduğu BGP tablosu (BGP Table), son olarak da BGP tablosundan alınan rotaların önerilen rota olup olmadığı kontrolü yapılarak tutulduğu, bir bakıma eleme işleminden sonra kalan networklerin tutulduğu IP Routing tablosudur. BGP daha sonra bu IP Routing tablosuna bakarak hangi networke nasıl ulaşacağını belirler.

2. BGP (Border Gateway Protocol - Sınır Geçiş Protokolü)



2. BGP (Border Gateway Protocol - Sınır Geçiş Protokolü)



3. CDP (Cisco Discovery Protocol - Cisco Tanımlama Protokolü)

- CDP, Cisco Discovery Protokol (Cisco Tanımlama Protokolü), Cisco cihazlarda kullanılan, bir cihaza direkt olarak bağlı olan komşu cihazları gösteren bir protokoldür. CDP; Yönlendirici , Anahtarlayıcı, Erişim Sunucusu (Access Server), Köprü gibi ağ cihazlarının hepsinde kullanılır. Bu protokol OSI, Open Systems Interconnection (Açık Sistemler Bağlantısı) modelinde ikinci katmanda (data link) kullanılan bir protokoldür.
- Bu protokol sayesinde ağ üzerinde bulunan bir cihazın komşu cihazlarının yerleri direk olarak tanımlanır. CDP kullanılarak sadece hangi cihaz olduğu değil aynı zamanda aygıt adı (device id), açık olan arayüzler (interface), cihazın portlarında bulunan ip adresleri, cihazların fonksiyonel kapasiteleri ve cihazların platformları, cihazda kullanılan işletim sistemi sürümü de rahatlıkla görülebilir.

3. CDP (Cisco Discovery Protocol - Cisco Tanımlama Protokolü)

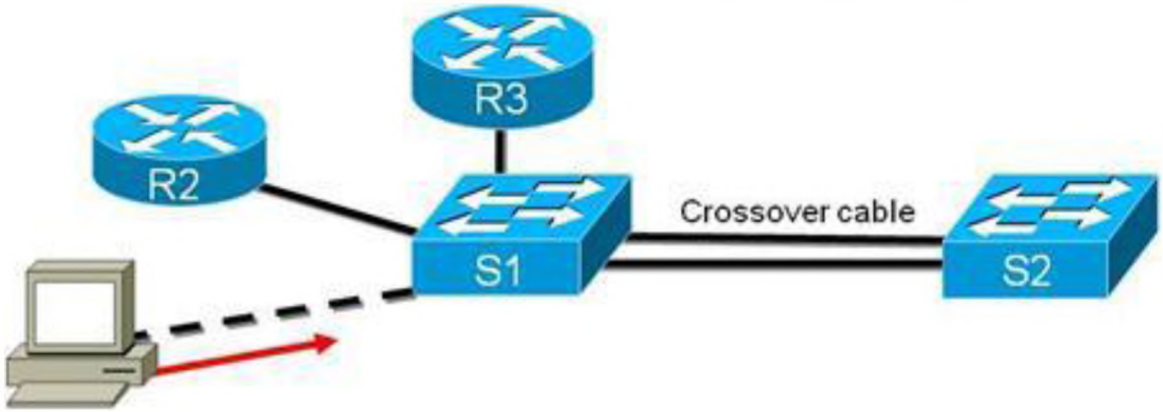
- Bu protokolün çalışma prensibi şu şekildedir; CDP'yi kapatılmamış olan her cihaz kendi ağında çoklu gönderim (multicast) olarak bilgilerini yayınlar. Bu şekilde diğer komşu cihazlar da bu bilgilere erişir. Fakat Cisco cihazlar bu bilgileri dinamik yönlendirme protokollerinde kullanılan tabloya yazmazlar. Yönlendirme protokollerinden elde ettikleri bilgiler için kullandıkları tablolar farklıdır.
- Cisco cihazlar CDP'den alacakları bu bilgilere ihtiyaç duymazlar. Bu protokol genel olarak ağı yöneten kişiler için faydalıdır. Ağ'da hangi cihazların hangilerine komşu olduğunu ve komşu cihazların bilgilerini ağ yöneticisi kullanır. Bu da ağı yönetirken ağ yöneticisine yardımcı olur.
- Özellikle küçük ağlarda CDP'nin ağ yöneticisi tarafından etkili kullanılması, dinamik yönlendirme protokollerine gerek kalmadan ağı yönetmeyi sağlar. Ağ topolojisi bilineceği için yönlendiricide yapılacak olan sabit yönlendirme işlemi ile yönlendiriciler haberleştirilebilir.

Cisco Discovery Protocol

show cdp neighbors

S1# **show cdp neighbor**

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
R2	Fas 0/1	170	R S I	Cisco 2811	Fas 0/0
R3	Fas 0/2	178	R	Cisco C804	Eth 0
S2	Fas 0/12	171	S I	WS-C3550-2	Fas 0/2
S2	Fas 0/11	171	S I	WS-C3550-2	Fas 0/1



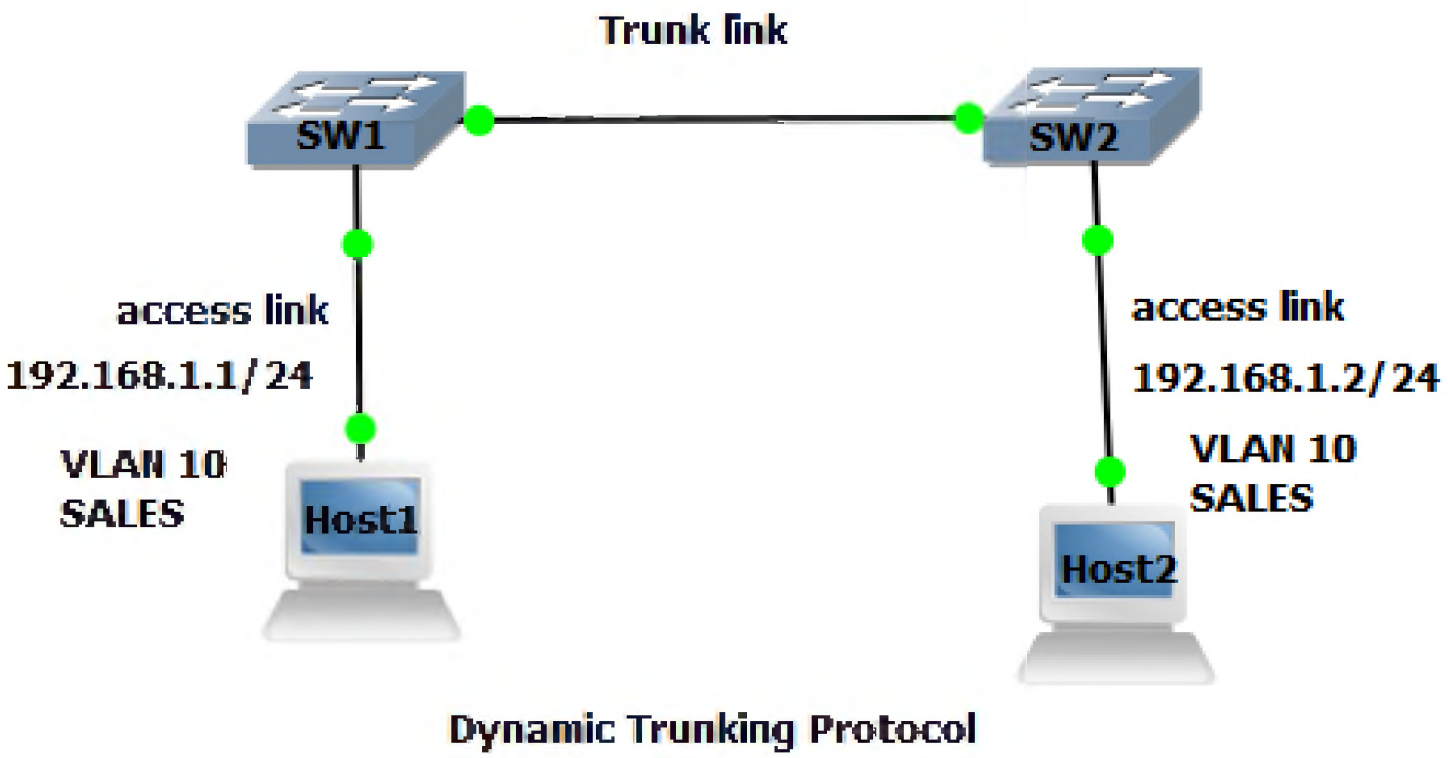
Who are your neighbors?

CertificationKits

4. DTP (Dynamic Trunking Protocol - Dinamik Gövdem Protokolü)

- **Dynamic Trunking Protocol (Dinamik Gövdem Protokolü)** Cisco tarafından geliştirilmiş OSI katmanlarından ikincisi olan "Data Link" katmanında çalışan ağ protokolüdür. DTP kısaca Cisco **Switchler (Anahtarlayıcılar)** arasında çalışan ve iki anahtarlayıcının aralarında paylaştıkları DTP mesajı ile, bağlı oldukları portu **Trunk portu (Gövde portu)** yapmasını sağlayan bir protokoldür.
- Dinamik Trunk Protokolü aracılığıyla portlar arası "trunk" olma işlemi otomatik olarak yapılmaktadır.
- Farklı vlan'lara sahip iki switch'in birbirine bağlanarak haberleşmelerini sağlamak için trunk işlemi yapılır.

Dynamic Trunking Protocol



5. GLBP (Ağ Geçidi Yük Dengeleme Protokolü)

- Ağda bulunan yönlendiricilerde bir sorun oluştuğunda yönlendirme işleminin devamlılığı yedeklilik protokolleriyle sağlanır.
- GLBP, Cisco firmasının geliştirmiş olduğu bir yedeklilik protokolüdür.
- GLBP'yi diğer dinamik gateway yedekliliği sağlayan protokollerden ayıran en büyük özelliği aktif olarak paket aktarımının yapıldığı birden fazla router'ın aynı anda çalışmasına imkan sağlamasıdır. GLBP bununla da kalmayıp aktif çalışan routerlar üzerinde istenilen düzeyde load-balancing yapılmasına da imkân sağlar.

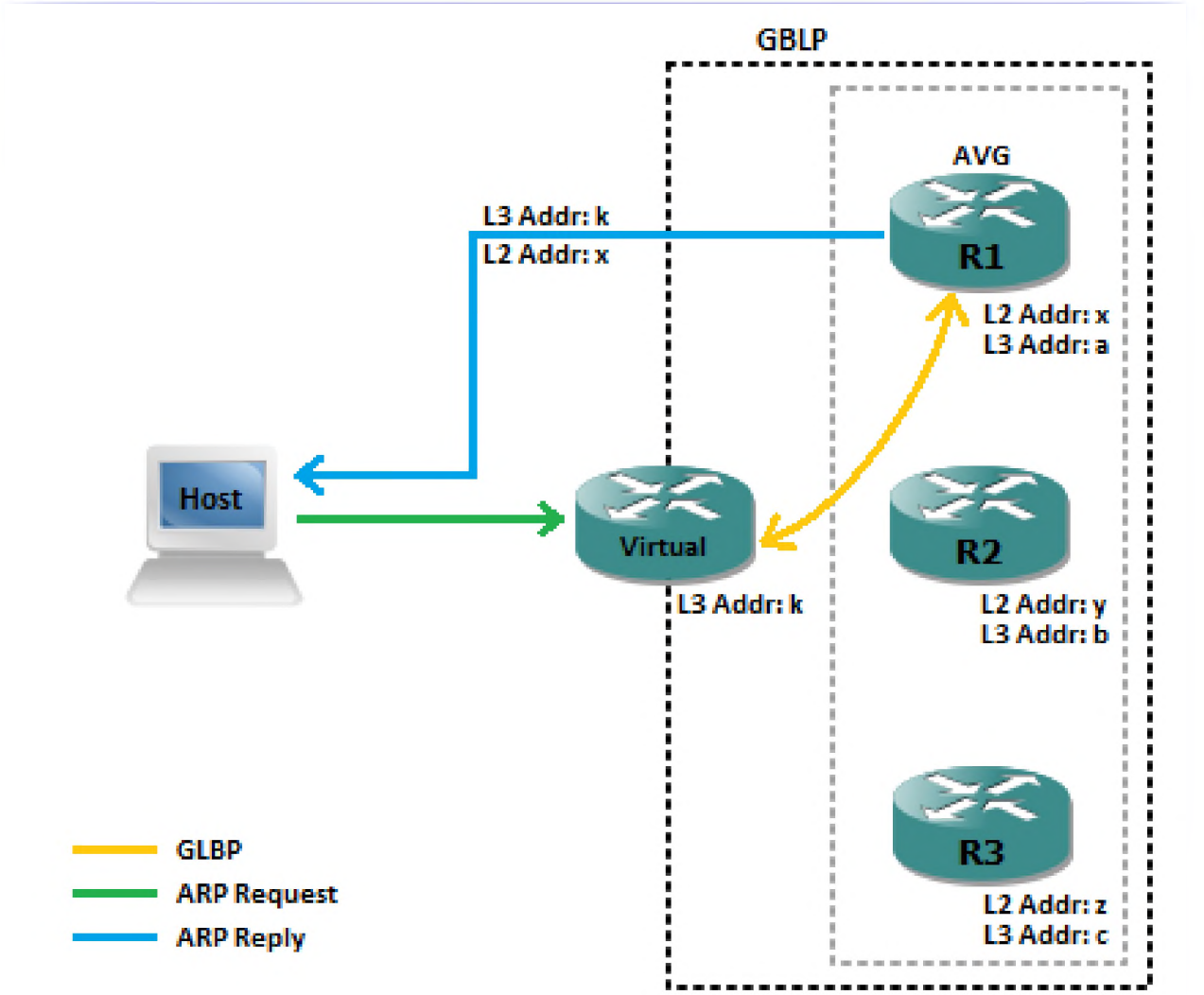
5. GLBP (Ağ Geçidi Yük Dengeleme Protokolü)

- GLBP tek bir sanal IP adresi kullanırken, birden fazla sanal MAC adresi kullanır ve bu kullanılarak yönlendiriciler arasında yük dengelemesi sağlanır.
- GLBP grubunda bir adet aktif yönlendirici (Active Virtual Router) seçilir yönlendiricilerden biri aktif modda iken diğeri ise bekleme modunda olur. Bu iki yönlendirici birbirlerine belli aralıklarla “hello” paketleri yollarlar. Eğer aktif olan yönlendirici ağ yöneticisi tarafından belirlenmiş sürede bir “hello” paketi yollamazsa beklemede olan yönlendirici aktif olan yönlendiricinin yerine geçer.

5. GLBP (Ağ Geçidi Yük Dengeleme Protokolü)

- Aktif yönlendirici diğer grup üyelerinin her birine eşsiz sanal bir MAC adresi verir. Bu grup üyeleri aktif sanal taşıyıcı (Active Virtual Forwarder) adını alırlar. Aktif yönlendirici gelen ARP isteklerine cevap vermekle yükümlüdür.
- Yük dengeleme, ARP isteklerine verilen cevaplardaki sanal MAC adresleriyle sağlanmaktadır.
- Aktif sanal taşıyıcılarda yedeklilik aktif sanal yönlendiricilerdekine benzerlik gösterir.
- GLBP gurubuna ait yönlendiricilerden bir kaçı aktif yönlendirici olarak seçilebilir.

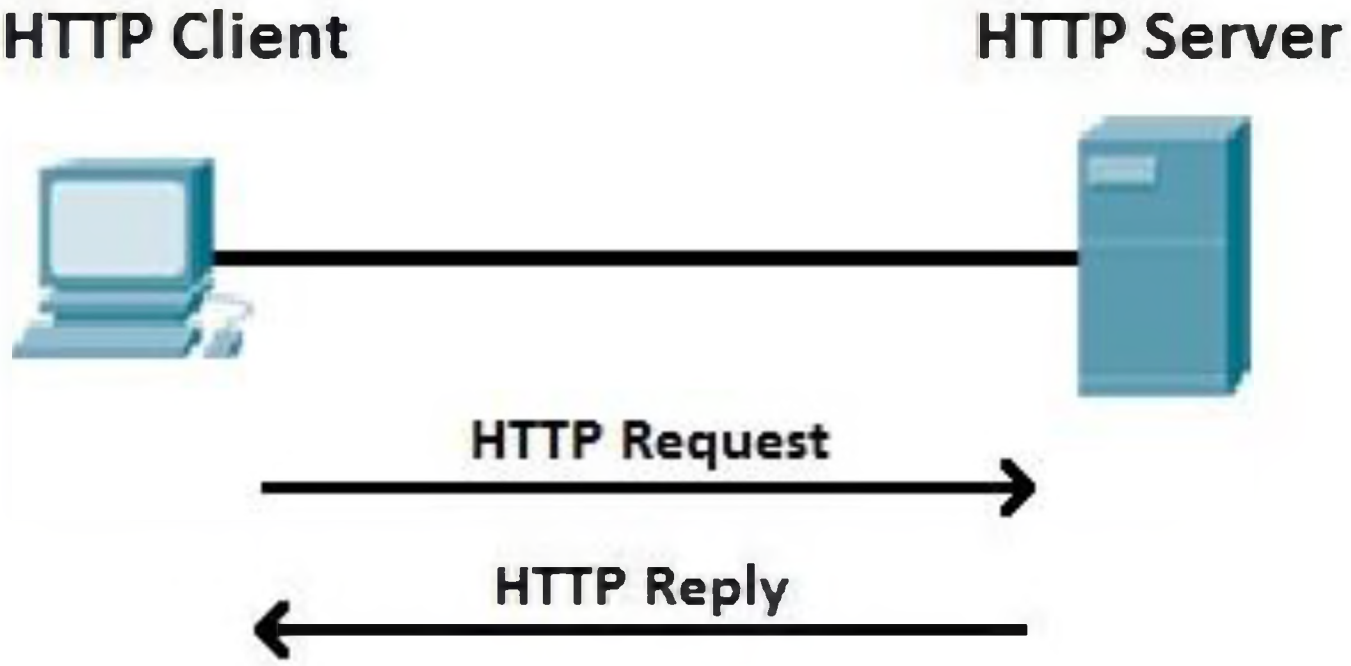
5. GLBP (Ağ Geçidi Yük Dengeleme Protokolü)



6. HTTP Protokolü

- HTTP, İnternette sunucular ve son kullanıcılar arasında bilgilerin nasıl aktarılacağına dair kurallar ve yöntemleri düzenleyen uygulama katmanında çalışan bir iletişim protokolüdür. Web sitesi görüntülemek ve üzerinde çeşitli işlemler yapmak için kullanılır.
- HTTP oturumu ağ üzerindeki "request-response" işleminin bir aşamasıdır. HTTP istemcisi istekte bulunur. İstemci belli bir port üzerinden TCP (Transmission Control Protocol – Aktarım Kontrolü İletişim Kuralı) bağlantısı kurar (Genellikle 80. porttan). O port üzerinde dinlemekte olan HTTP sunucusu istemcinin istek mesajını bekler. İstek ulaştığında sunucu durum sinyalini gönderir. Sinyalde örnek olarak “HTTP/1.1 200 OK” ve ardından muhtemelen istenilen kaynağın gövde metni, hata mesajı veya bazı diğer bilgiler bulunabilir.

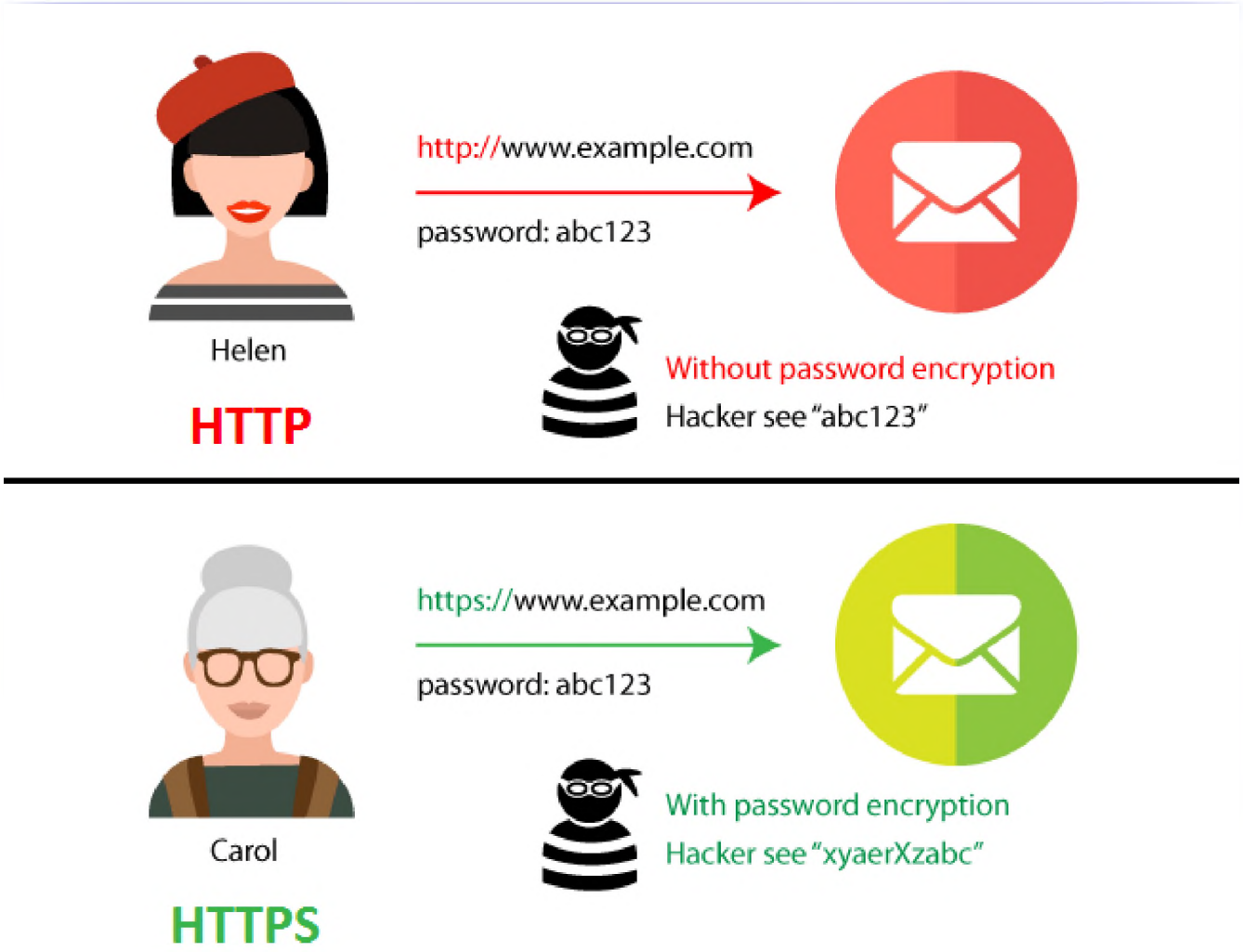
HTTP Protokolü



6. HTTPS Protokolü

- HTTPS, HTTP ile SSL/TLS (Secure Sockets Layer / Transport Layer Security – Güvenli Soket Katmanı / Aktarım Katmanı Güvenliği) iletişim kurallarının şifrelenmiş iletişim ve güvenli tanımlama amacıyla birleşimidir. Varsayılan olarak 443'üncü porttan bağlantı kurar.
- HTTPS'in asıl amacı güvenli olmayan bir iletişim ağı üzerinden güvenli bir kanal oluşturmaktır. Bu yöntem hattı dinlemek isteyenlere karşı yeterli korumayı da sağlar. Banka Web-sayfaları veya yüksek güvenlik gerektiren uygulamalarda tercih edilir.

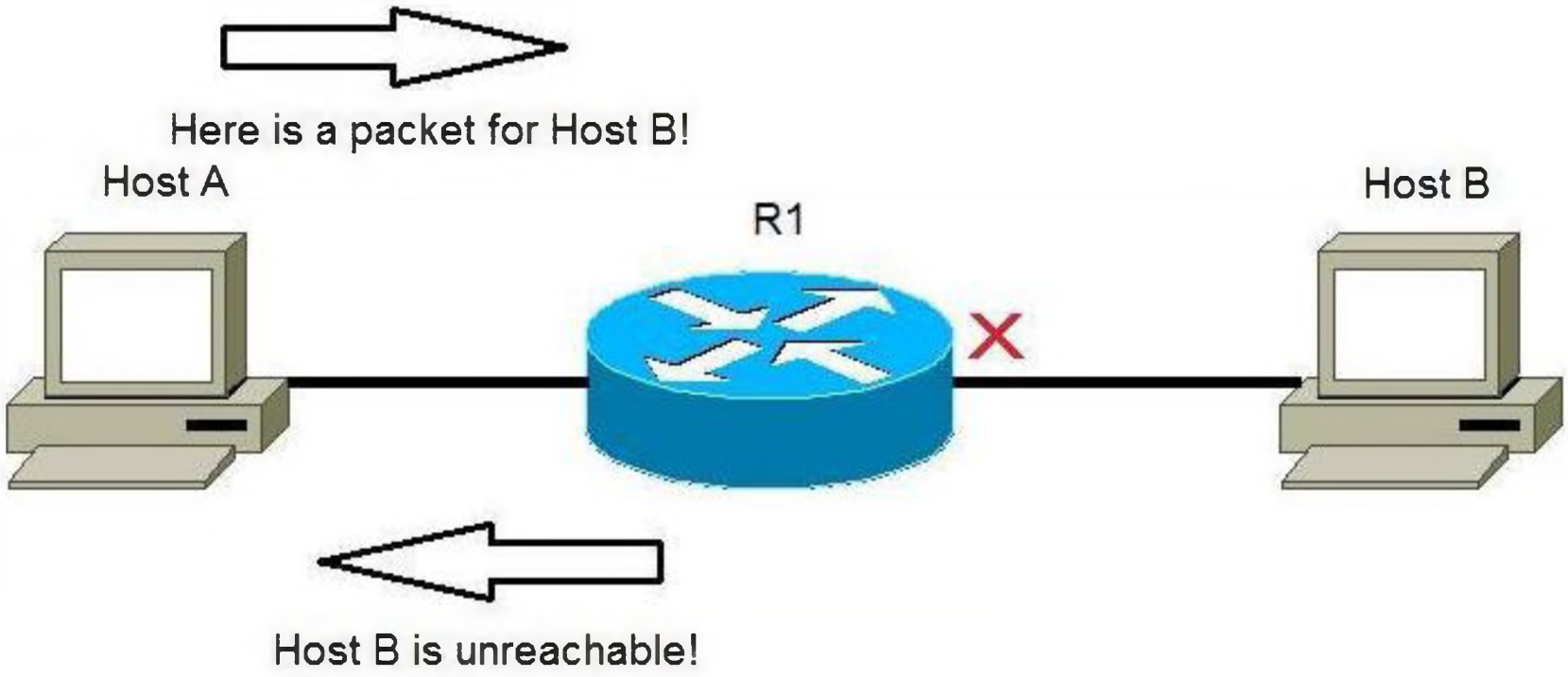
HTTPS Protokolü



7. ICMP (Internet Control Message Protocol)

- TCP/IP protokol takımında, İnternet Protokolü (IP) bilgisayarlar arasında veya ağ geçitlerinde hata raporlama, hata düzeltme ya da durum bildirme yeteneklerine sahip değildir.
- ICMP, İnternet Katmanında IP paketinin veri bölümünde çalışıp, sorunları haberleşen birimlere bildirerek bir geri besleme mekanizması oluşturur.
- ICMP genel olarak; TTL süresi dolduğu zaman paketin sahibine bildirim yapma, herhangi bir durumda yok edilen paket hakkında geribildirim sağlama, hata oluşumlarında geribildirim sağlama, paket başka bir yoldan gideceği zaman geribildirim sağlama gibi görevler üstlenir.
- Örneğin, sorun çözümü için sıkça kullanılan Ping ve Tracert komutları ICMP Echo Request ve ICMP Echo Reply mesajları ile çalışır.

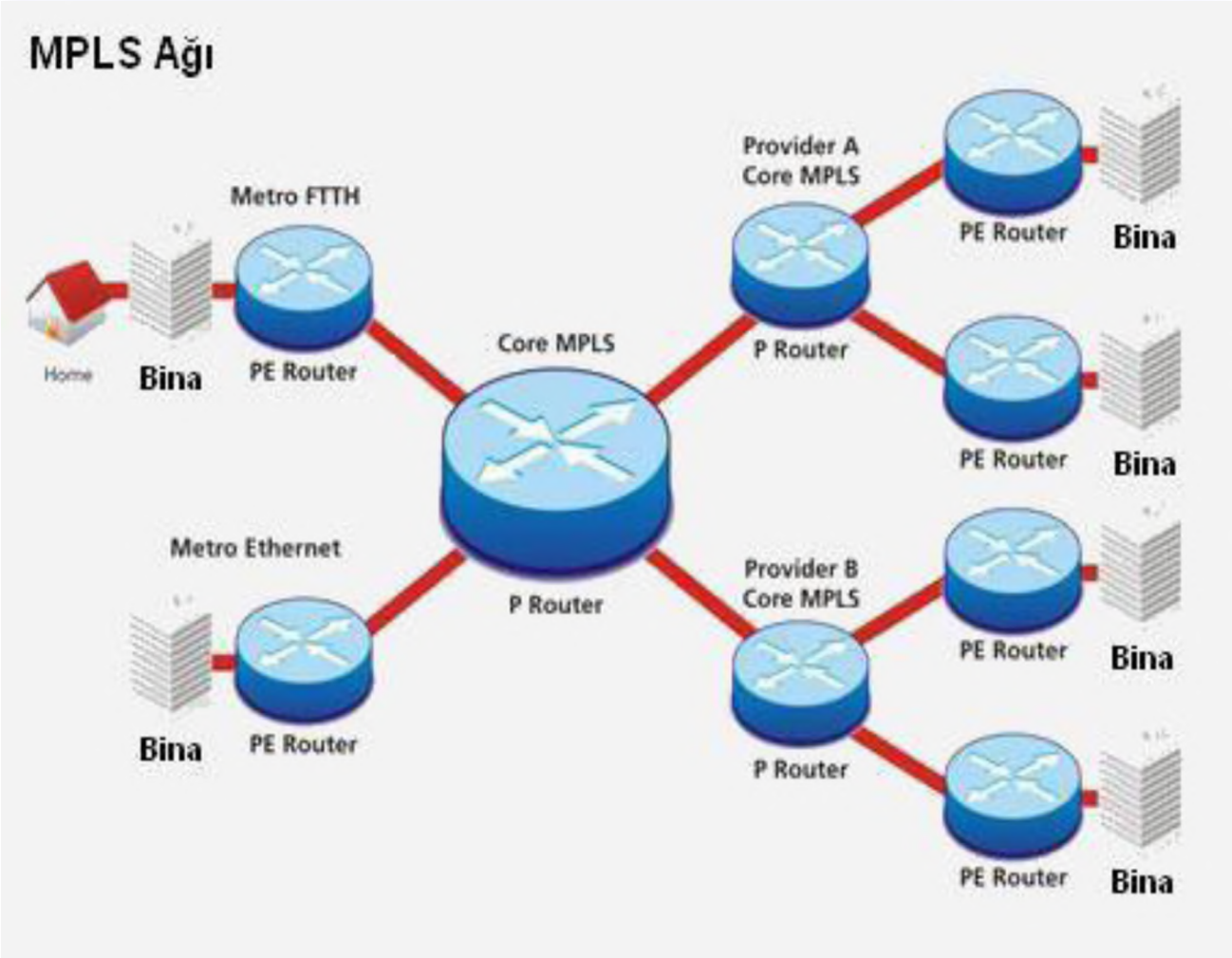
Internet Control Message Protocol



8. MPLS (Multi Protocol Label Switching - Çoklu Protokol Etiket Anahtarlama)

- Çoklu protokol etiket anahtarlama **(MPLS)** yüksek performanslı ağlarda bir bilginin bir ağ düğümünden diğerine aktarılmasını sağlayan bir mekanizmadır. MPLS uzak iki düğüm arasında sanal bağlantı kurulumunu kolaylaştırır. Değişik ağ protokollerine ait paketlerin sarmalanmasını sağlar.
- MPLS **"Paket Anahtarlama Ağları"** ailesinin bir üyesidir. Bu mekanizma herhangi bir OSI Model katmanında çalışabilir. Genelde geleneksel olan 2. katman ve 3. katman arasında kullanılır ve bu yüzden **2.5'uncu katman protokolü** olarak adlandırılır. Devre temelli kullanıcılar ve paket anahtarlama temelli kullanıcılara yönelik birleşmiş bir bilgi taşıma sistemi kurulması amacıyla kullanılan bir datagram servis modelidir. IP paketleri ve doğal ATM, SONET ve Ethernet çerçeveleri dahil olmak üzere birçok değişik trafiğin taşınmasında kullanılabilir.

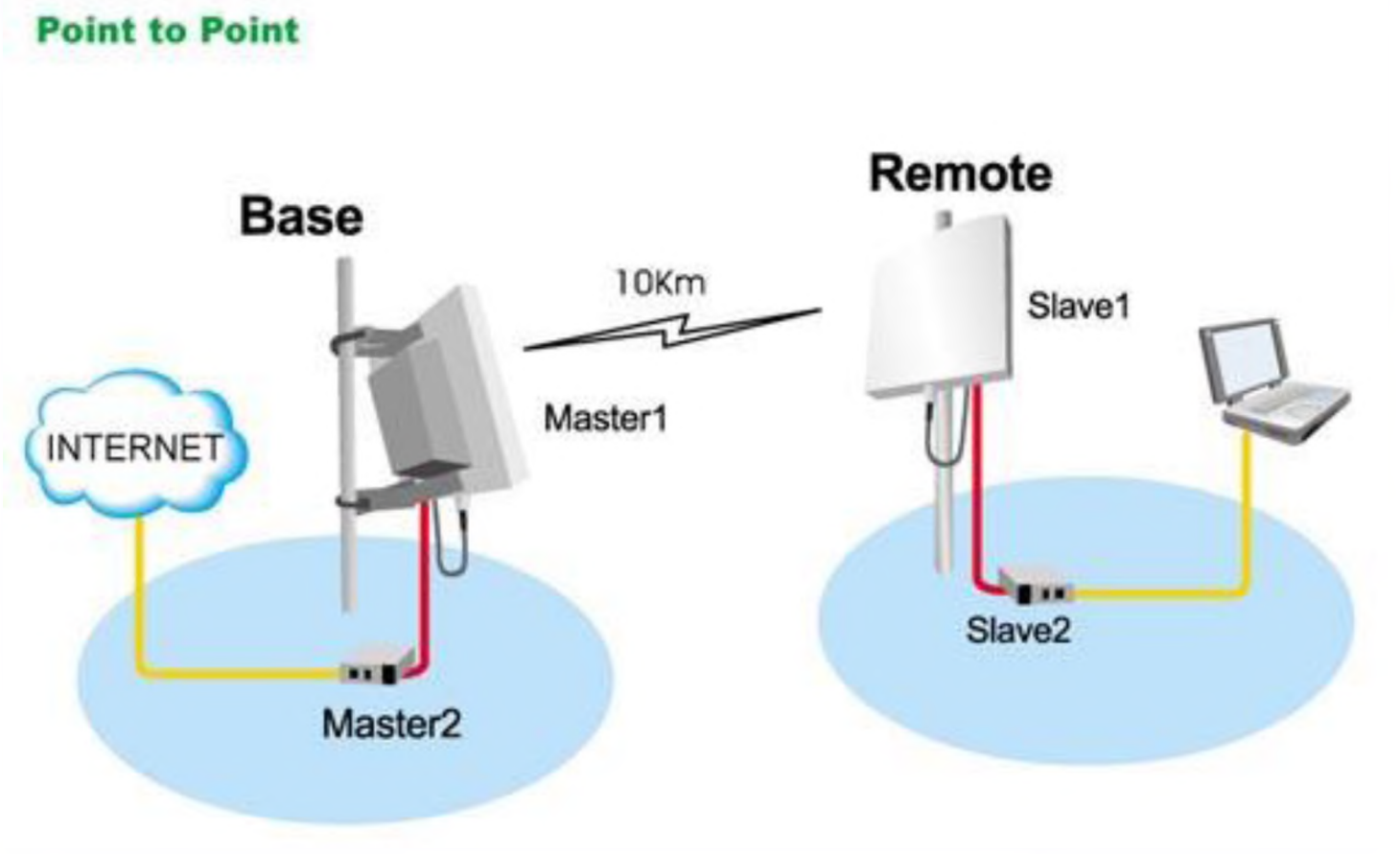
8. MPLS (Multi Protocol Label Switching - Çoklu Protokol Etiket Anahtarlama)



9. Point to Point Protocol (Noktadan Noktaya Protokolü)

- PPP (Point to Point Protokolü) bir Veri Bağlama Katmanı (Data Link Layer) protokolüdür ve veri alışverişi yapmak isteyen iki noktanın, telefon hattı gibi seri bir hat üzerinden bağlantısını sağlayarak çift yönlü iletim (full-duplex) yapılabilmesine olanak sağlar. Bu nedenle bu protokolün kullanıldığı noktadan noktaya bağlantılar çift yönlü iletimi destekleyecek nitelikte olmalıdır.
- PPP Protokolü, **"Seri Hat Üzerinden İnternet Protokolü"** olarak adlandırılan **SLIP (Serial Line IP)** protokolünün sıkıştırma ve düzenleme özelliklerinin geliştirilmesiyle ortaya çıkmış standart iletişim kuralları kümesidir. Her iki protokol de **TCP/IP (İnternet Protokolleri Ailesi)** için geliştirilmiş **Geniş Alan Bağlantısı (WAN)** protokolleridir ve modem ya da benzer başka bir cihaz yardımıyla seri bağlantılar kurulmasına olanak sağlarlar.

Point to Point Protocol

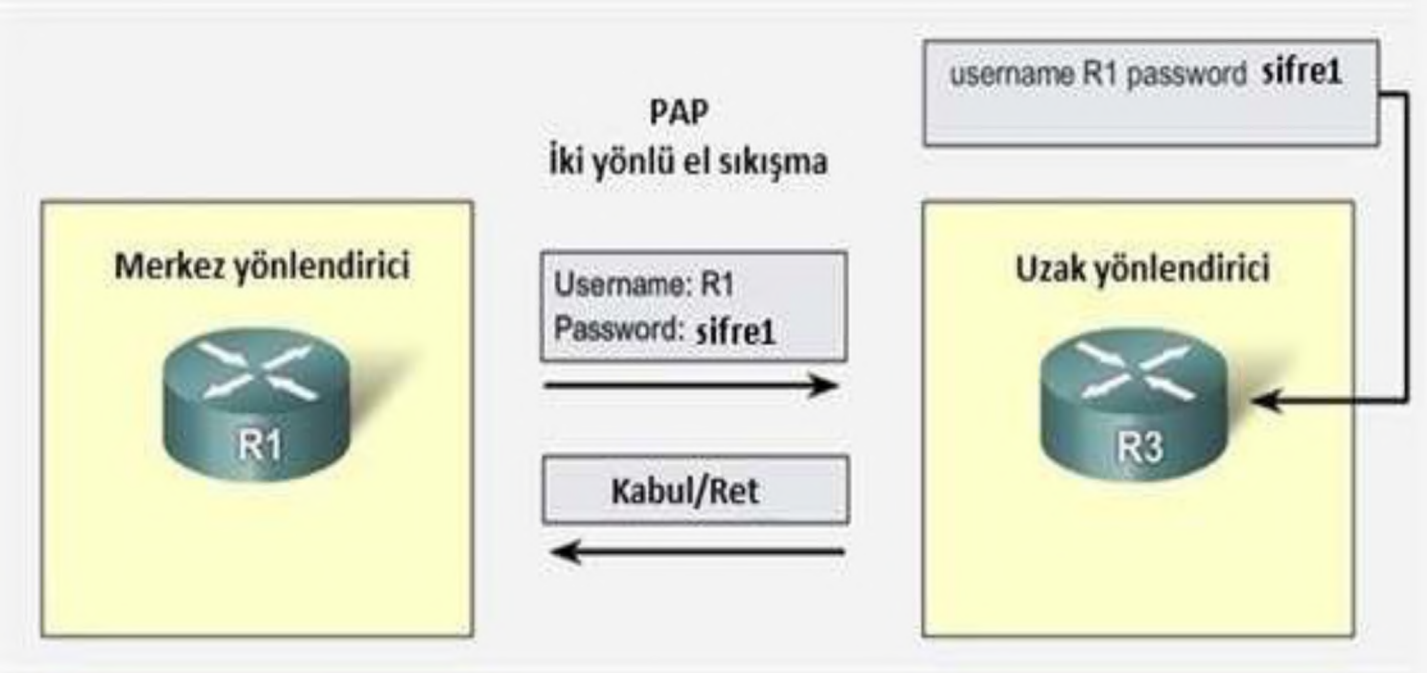


10. PPP (Noktalar Arası İletişim Kuralı) Kimlik Doğrulama Metodları

- PAP (Password Authenticaton Protocol - Şifre Doğrulama Kuralı)
- CHAP (Challenge Handshake Authentication Protocol - Üçlü El Sıkışma Kimlik Doğrulama Kuralı)

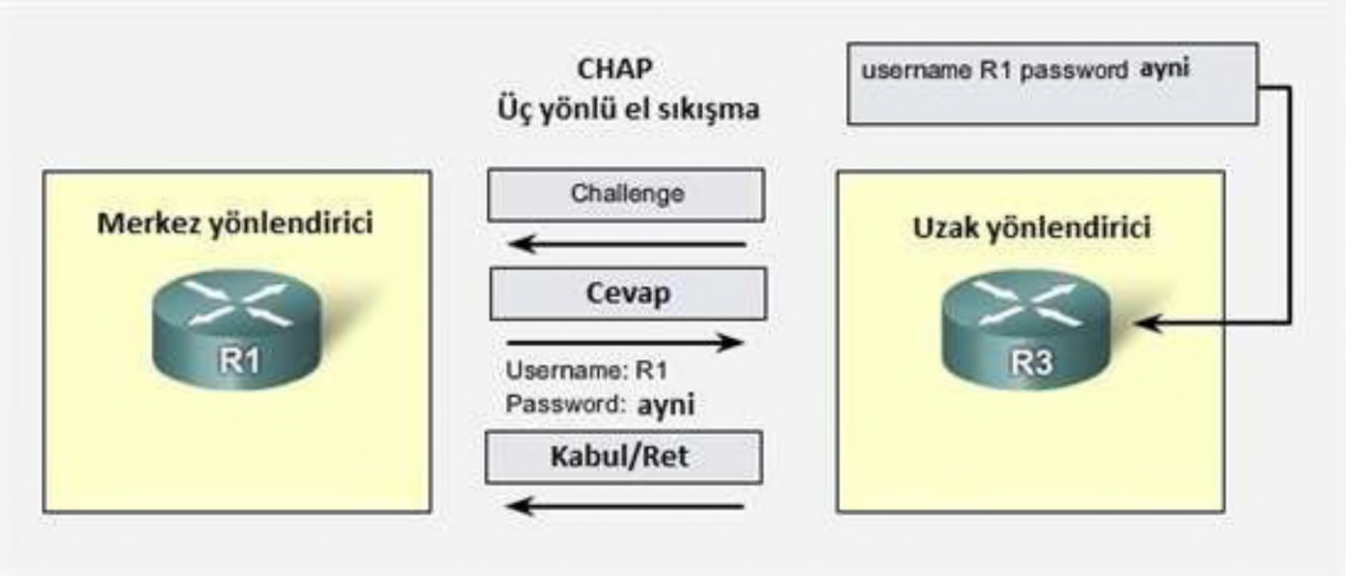
10. PPP (Noktalar Arası İletişim Kuralı) Kimlik Doğrulama Metodları

- **2-Way Handshake (İki Yönlü El Sıkışma)** Kullanıcı adı ve şifre bu yöntemde şifreleme yapılmadan, açık olarak karşı tarafa ulaştırılır. PAP'ta bağlantı kurulduktan sonra bir daha kimlik denetimi yapılmaz. Ayrıca PAP'ta şifrelerin aynı olma zorunluluğu yoktur.



10. PPP (Noktalar Arası İletişim Kuralı) Kimlik Doğrulama Metodları

- **3-Way Handshake (Üç Yönlü El Sıkışma)** yapar. Kimlik denetimi açık olarak yapılmaz, md5 matematik fonksiyonuna tabi tutularak "hash" (geri dönüşü olmayan fonksiyon) haline getirilir. Ayrıca CHAP'ta kimlik doğrulama belirli aralıklarla yapılır. Bütün bu özellikleri CHAP'ı PAP'tan daha güvenli bir protokol yapmaktadır.



11. SIP (Session Initiation Protocol - Oturum Başlatma Protokolü)

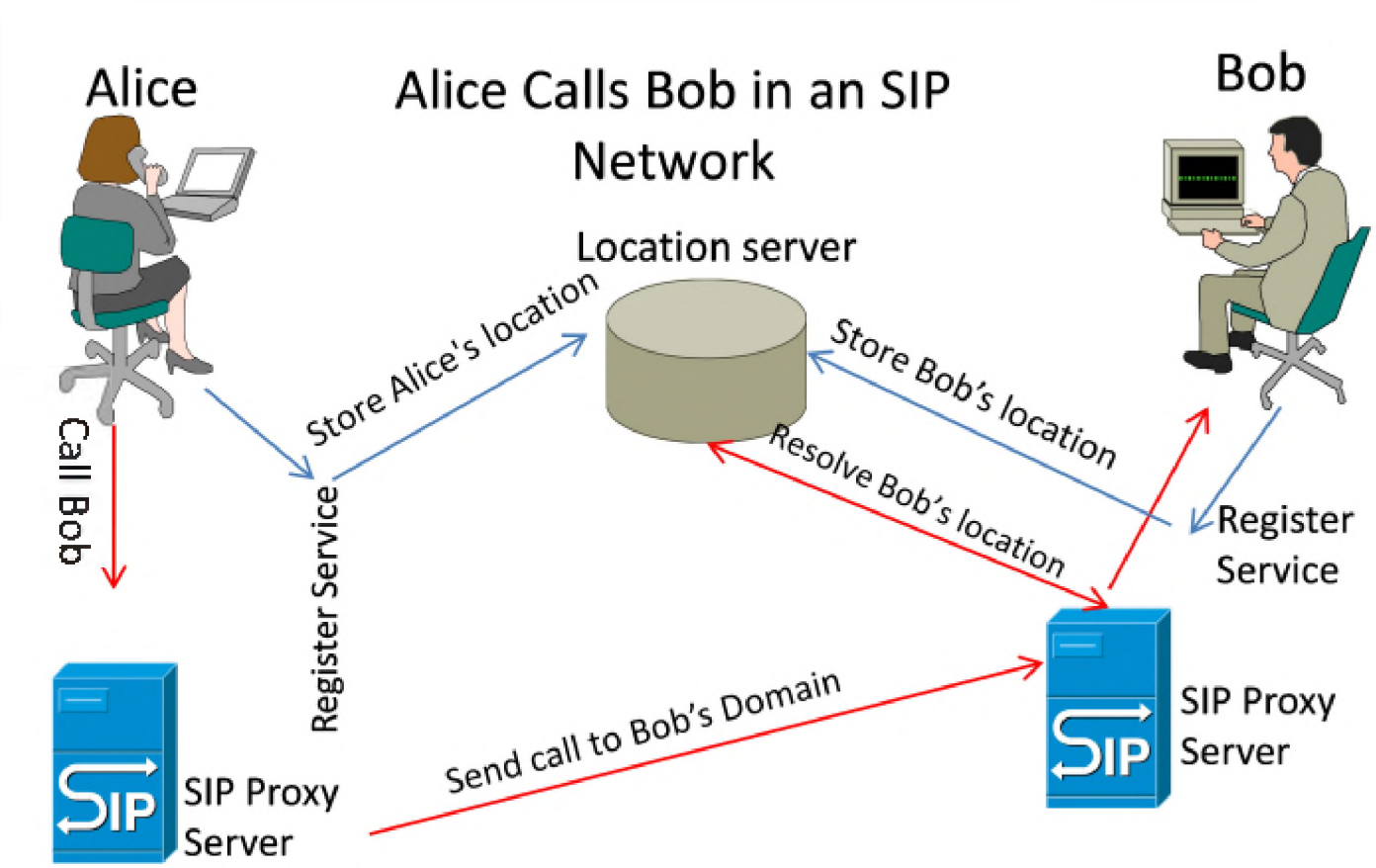
- **SIP (Session Initiation Protocol - Oturum Başlatma Protokolü)** iki ya da daha fazla katılımcı arasında bağlantı kuran, oturum başlatan ve gerçek zamanlı protokoller aracılığıyla veri taşınmasını sağlayan bir ağ protokolüdür.
- SIP, ağ üzerinden telefon görüşmeleri başta olmak üzere ses ve görüntü gibi çoklu ortam aktarımında oturum başlatmak için yaygın olarak kullanılır.
- Veri aktarımı ise **RTP (Real Time Protokol - Gerçek Zamanlı Protokol)** aracılığıyla sağlanır.

11. SIP (Session Initiation Protocol - Oturum Başlatma Protokolü)

SIP protokolü genel olarak;

- Bağlantı kurulmak istenen katılımcının adresini saptar ve adres çözümlemesi yapar.
- Bağlantı kurulmak istenen katılımcının uygun olup olmadığını belirler ve katılımcılar arasında oturum başlatır.
- Bağlantı kurulan katılımcıların desteklediği çoğul ortam türlerini belirler ve katılımcılara göre optimal olan çoğul ortamı seçer. Örneğin; ikiden çok katılımcı arasında kurulan bağlantılarda veri, SIP'in belirlediği ve tüm istemciler tarafından ortak olarak desteklenen çoklu ortam türünde aktarılır.
- Katılımcılar arasında oturum başladıktan sonra, yeni katılımcının bağlanması ya da var olan katılımcının ayrılması gibi işlemleri yönetir. Oturumların sonlandırılmasını sağlar.

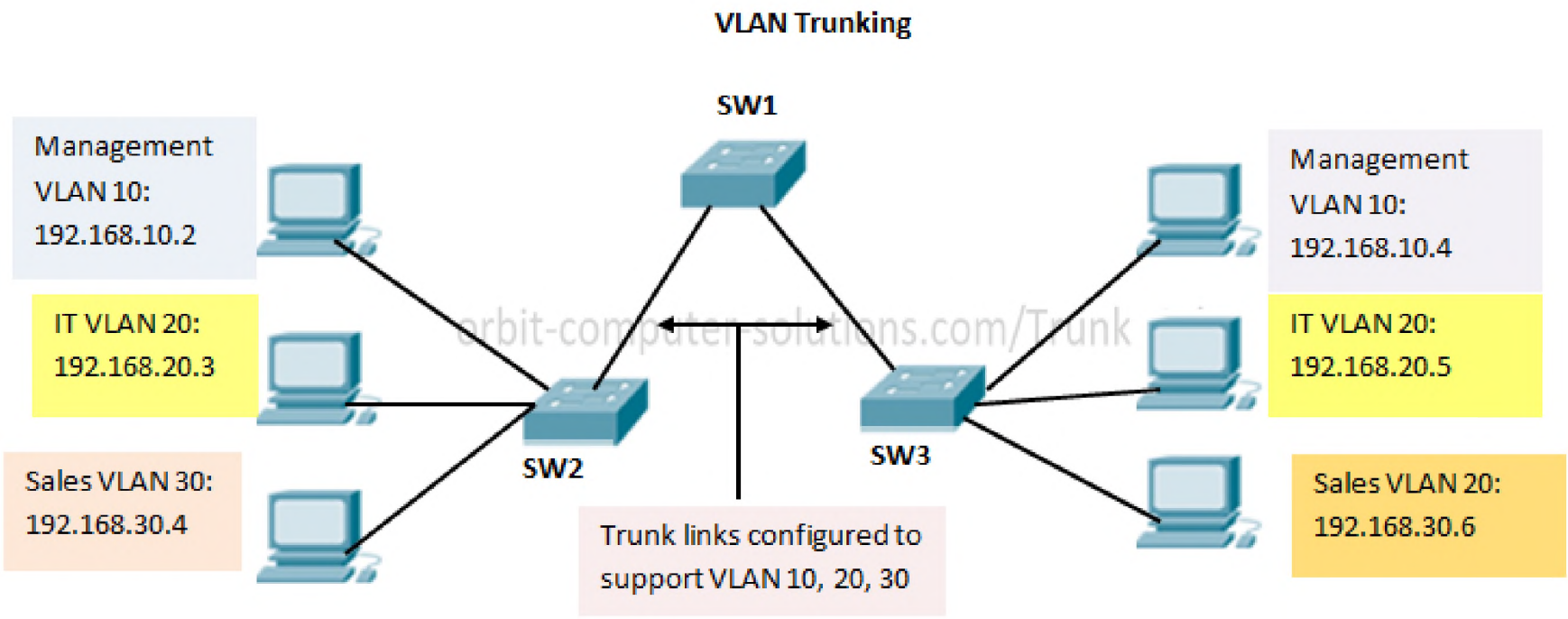
Session Initiation Protocol



12. VTP (VLAN Trunking Protocol)

- VLAN Trunk Protokolü bir networkte yeni VLAN'lar eklenmesi, mevcut VLAN'ların silinmesi ve yeniden adlandırılması işleminin tek elden yönetilmesini sağlayan Cisco tabanlı bir 2. Katman protokolüdür. Bu protokol kullanılarak ağ üzerindeki yönetim daha etkili ve kolay bir şekilde sağlanmış olur.
- Genel olarak server olarak tanımlanmış bir switchte yapılan VLAN konfigürasyonunu bu switch ile aynı VTP domaininde bulunan tüm switchlere yayarak network yöneticisini ağdaki tüm switchlere ayrı ayrı VLAN konfigürasyonu yapma zahmetinden kurtarır ki bunların sayısı yüzlerce olabilir.

VLAN Trunking

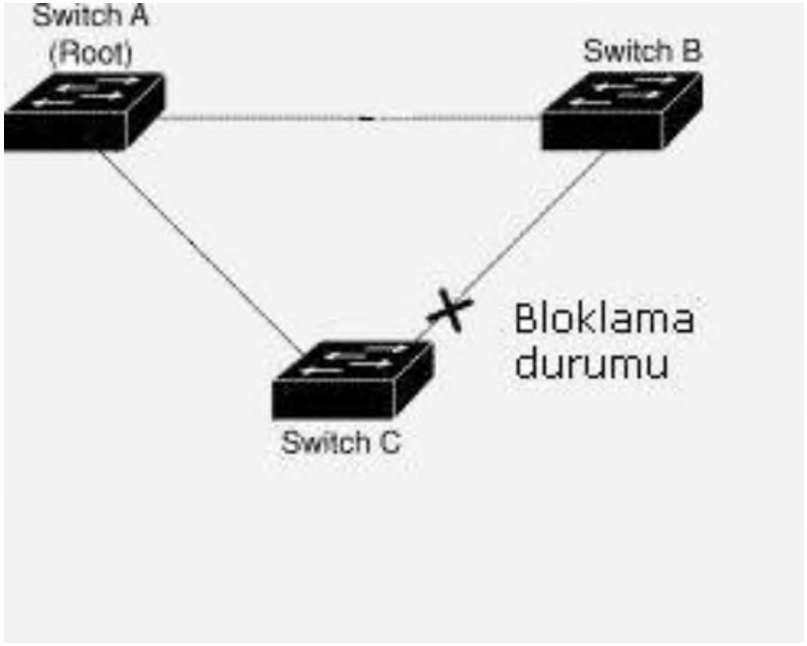


13. Spanning Tree Protokolü (STP)

- Spanning Tree Protokolü (STP), bir IEEE 802.1 standardıdır.
- Gereğinden fazla fiziksel bağlantıya sahip ağlarda anahtarlayıcı da dahil olmak üzere tüm köprü (bridge) cihazlarında yazılım bazında spanning-tree algoritması kullanarak herhangi bir LAN segmenti (çarpışma etki alanı) arasında sadece tek bir aktif bağlantı kalması için bazı portları bloklar.
- Aynı zamanda duraklar arasında birden çok aktif yol bulunmasıyla meydana gelebilecek döngüleri de engeller.

13. Spanning Tree Protokolü (STP)

- Spanning-tree algoritması, köprü ve anahtarlayıcı temelli ağlarda kullanılır ve trafiğin kaynaktan hedefe giderken geçebileceği en iyi yola karar verir. Bu algoritma tüm yedek yolları da göz önünde bulundurup, herhangi bir anda bunlardan yalnızca birini aktif hale getirir.

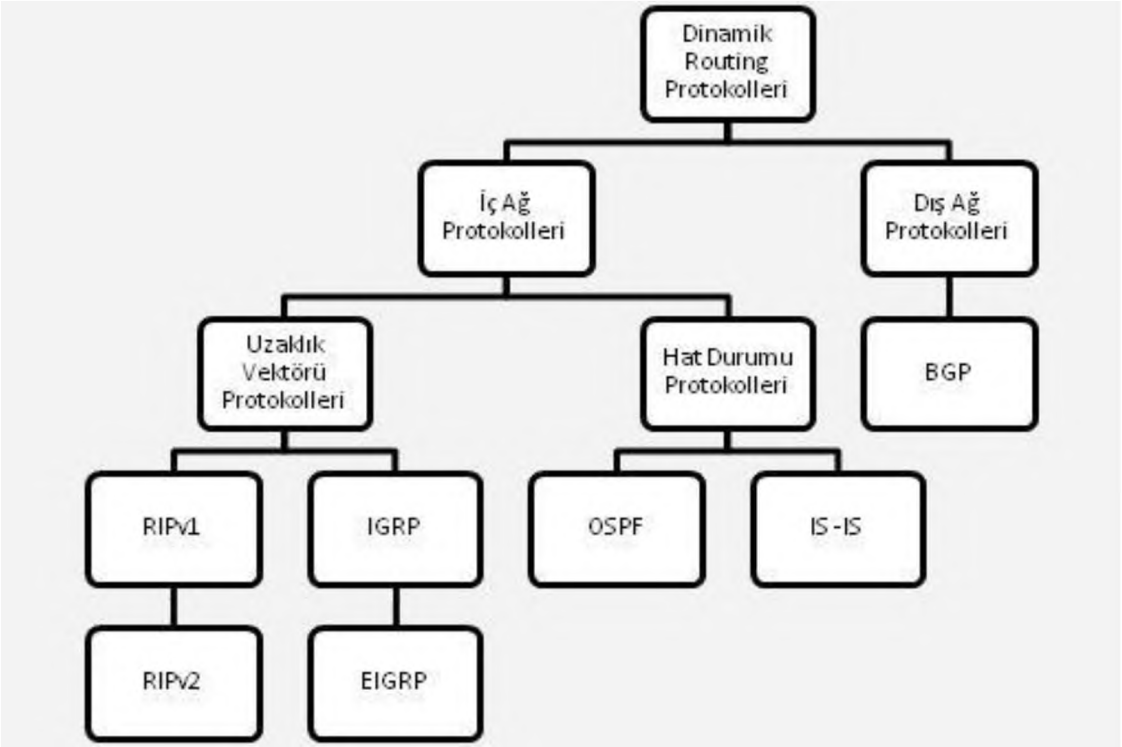


14. Yönlendirme (Routing) Protokolleri

- Yönlendirici üzerinde çalışan ve tablonun güncellenmesini sağlayan kurallardır; genelde yazılım ile gerçekleştirilirler.
- Protokoller iç (interior) ve dış (exterior) olarak iki sınıfa ayrılmıştır. İç protokoller daha çok pek fazla büyük olmayan özel ağ içindeki yönlendiriciler arasında kullanılırken, dış protokoller birbirinden bağımsız ve geniş ağlar arasındaki yönlendiriciler üzerinde kullanılır.
- Yönlendirme protokolleri (routing protocols ile yönlendirmeli protokoller (routed protocols), genelde birbiriyle karıştırılır; ancak farklı tanımlamalardır.

14. Yönlendirme (Routing) Protokolleri

- Farklı ağları haberleştirmek için kullanılan routing (yönlendirme) protokolleri, statik ve dinamik olmak üzere iki farklı yöntem kullanırlar. Dinamik routing yapan protokoller aşağıdaki şemayla özetlenebilir:



14. Yönlendirme (Routing) Protokolleri

- IGP (Interior Gateway Protocol)
- RIP (Routing İnformation Protocol)
- OSPF (Open Shorthest Path First)
- EGP (Exterior Gateway Protocol)
- EGP2 (Exterior Gateway Protocol 2)
- BGP (Border Gateway Protocol)

14. Yönlendirme (Routing) Protokolleri

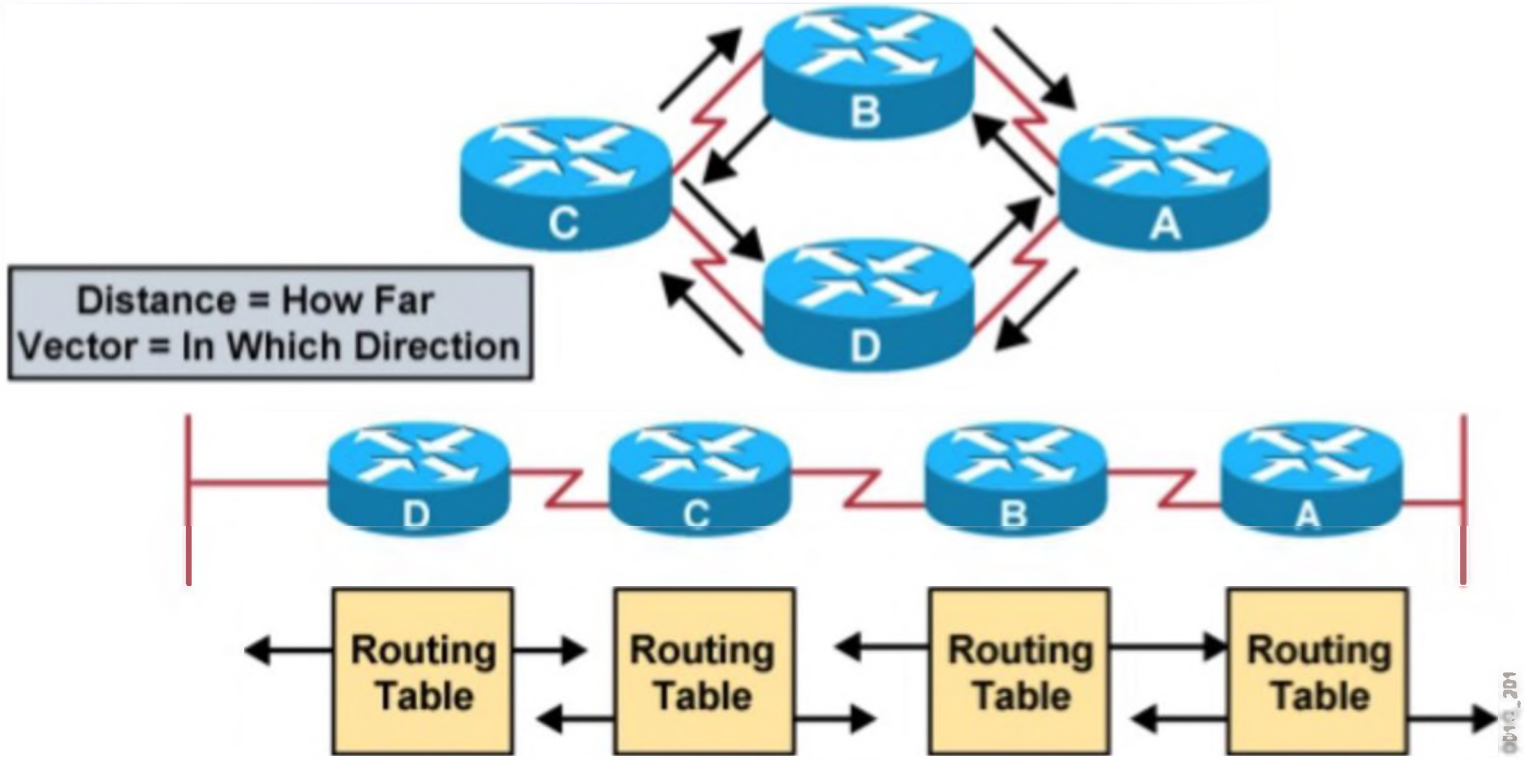
Uzaklık Vektörü Protokolleri (Distance Vector Protocol):

- Bu protokollerde rotalar uzaklık ve doğrultu vektörlerine bağlı olarak belirlenir. Uzaklık, geçilen hop (durak) sayısına göre; doğrultuda bir sonraki hoba ya da çıkış interface (arabirim)'ine göre belirlenir. Uzaklık Vektörü Protokolleri, en iyi rotayı belirlemek için Bellman-Ford algoritmasını kullanırlar.
- Bellman-Ford algoritması, ulaşılabilen ağların bilgilerini veritabanında tutmaya imkan sağlasa da; komşu routerın gönderdiği kadar bilgi sahibi olunduğundan, herhangi bir router, tüm topolojinin haritasına sahip değildir. Bu protokollerde router, tablodaki kaydın sadece bir bölümü değişse bile, tüm routing tablosunu periyodik olarak komşularına gönderir.

14. Yönlendirme (Routing) Protokolleri

- Bu durum, büyük ağlarda önemli bir trafiğe neden olur. Ayrıca, paketler gönderilirken üzerinde değişiklik yapıldığından, güncelleme yavaş gerçekleşir.
- Uzaklık vektörü protokolleri, en iyi yolu seçerken basit algoritmalar kullandıklarından, routerın işlemcisine fazla yük bindirmezler; ancak bazen en doğru yolu seçemeyebilirler.
- Bu protokoller; özel hiyerarşik bir düzen gerektirmeyen basit ağlarda, hub-and-spoke (merkezdeki router'ın diğerlerine hizmet verdiği yapı) gibi bazı özel ağlarda ve konverjans (topolojideki bütün routerların bütün ağları öğrenmesi) süresinin önemli olmadığı durumlarda tercih edilir.

Distance Vector Protocol



- Routers pass periodic copies of their routing table to neighboring routers and accumulate distance vectors.

14. Yönlendirme (Routing) Protokolleri

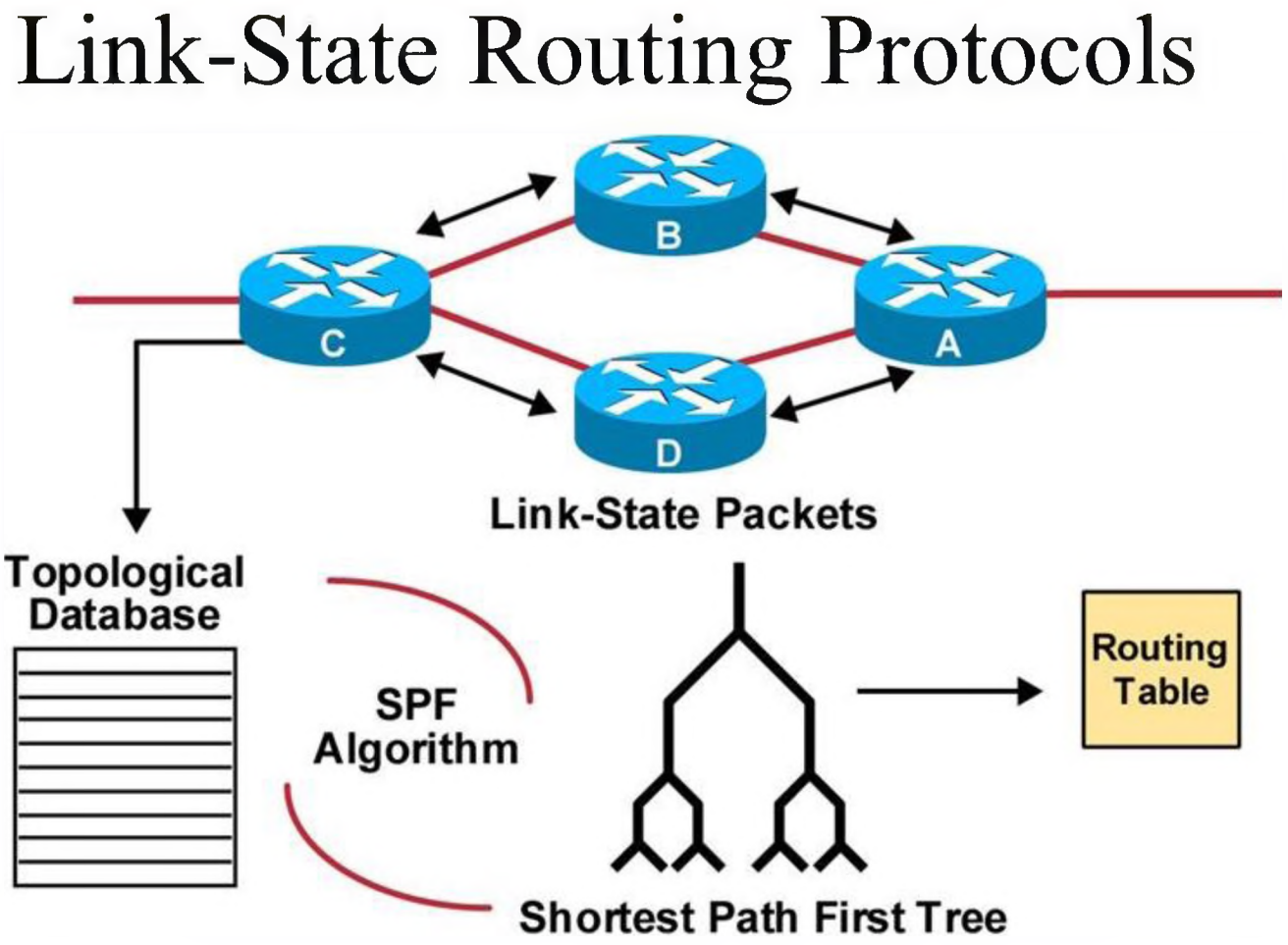
Hat Durumu Protokolleri (Link State Protocol):

- Bu protokollerle çalışan routerlar, diğer routerlardan öğrendikleri bilgiler sayesinde, tüm ağın topoloji haritasını çıkarabilirler. Yani iki nokta arasındaki tüm yolların bilgisine sahiptirler. Böylece tüm alt ağları bir ağaçta toplayıp, Shortest Path First (Önce En Kısa Yol) algoritmasıyla hangi yoldan gidileceğine dair en doğru kararı verirler.
- Ayrıca topoloji bir kez oturunca, periyodik güncellemeler yerine, sadece değişiklik olduğunda, küçük paketlerle güncelleme yapılır ve bu da trafik oluşmasını engeller.
- Paketler, üzerinde herhangi bir değişiklik yapılmadan komşu routera aktarıldığından, uzaklık vektörü protokollerinde karşılaşılan hız sorunu bu protokollerde yoktur.

14. Yönlendirme (Routing) Protokolleri

- Ancak karmaşık ve çok parametreli algoritmalar kullandıklarından, uzaklık vektörü protokollerine kıyasla daha güçlü bir işlemci ve ram'e ihtiyaç duyarlar. Önceleri bu durum ekonomik bir dezavantaj olarak görünse de, günümüzde işlemci ve ram fiyatları düştüğünden, önemli bir dezavantaj olmaktan çıkmıştır.
- Hat Durumu Protokolü, hiyerarşik yapılı büyük ağlarda ve konverjans süresinin kısalığının önemli olduğu durumlarda tercih edilir.

Link State Protocol



15. NAT (Network Address Translation - Ağ Adresi Çeviricisi)

- NAT bir ağda bulunan bilgisayarın, kendi ağı dışında başka bir ağa veya İnternete çıkarken farklı bir IP adresi kullanabilmesi için geliştirilmiş bir İnternet protokolüdür. Yani NAT bilgisayarın sahip olduğu IP adresini istenilen başka bir adrese dönüştürür.
- Bilindiği gibi Ipv4'te her IP adresi kullanılabilir durumda değildir. Ipv4'te kullanılabilir durumda olan IP'lere bakıldığında yaklaşık olarak 3,2 milyar kadar IP bulunmaktadır. Bu IP sürümünün yaratabileceği IP yetersizliği göz önüne alınarak NAT protokolü geliştirilmiştir. İnternette bazı adresler yerel ağlarda kullanılmak amacıyla özel adresler (private IP address) olarak ayrılmıştır. Bu özel adresler:

15. NAT (Network Address Translation - Ağ Adresi Çeviricisi)

- 10.0.0.0/8 -> 10.0.0.0 - 10.255.255.255
  172.16.0.0/12 -> 172.16.0.0. - 172.31.255.255
  192.168.0.0/16 -> 192.168.0.0 - 192.168.255.255 arasındadır.
- Dünya üzerinde birçok şirket ve kurum yerel ağlarında yukarıda verilen özel IP'leri kullanmakta, dış bağlantılarını ise NAT yapabilen uygun yönlendiriciler (router) kullanarak, IP adreslerini genel adreslere (public address) çevirerek sağlamaktadırlar.

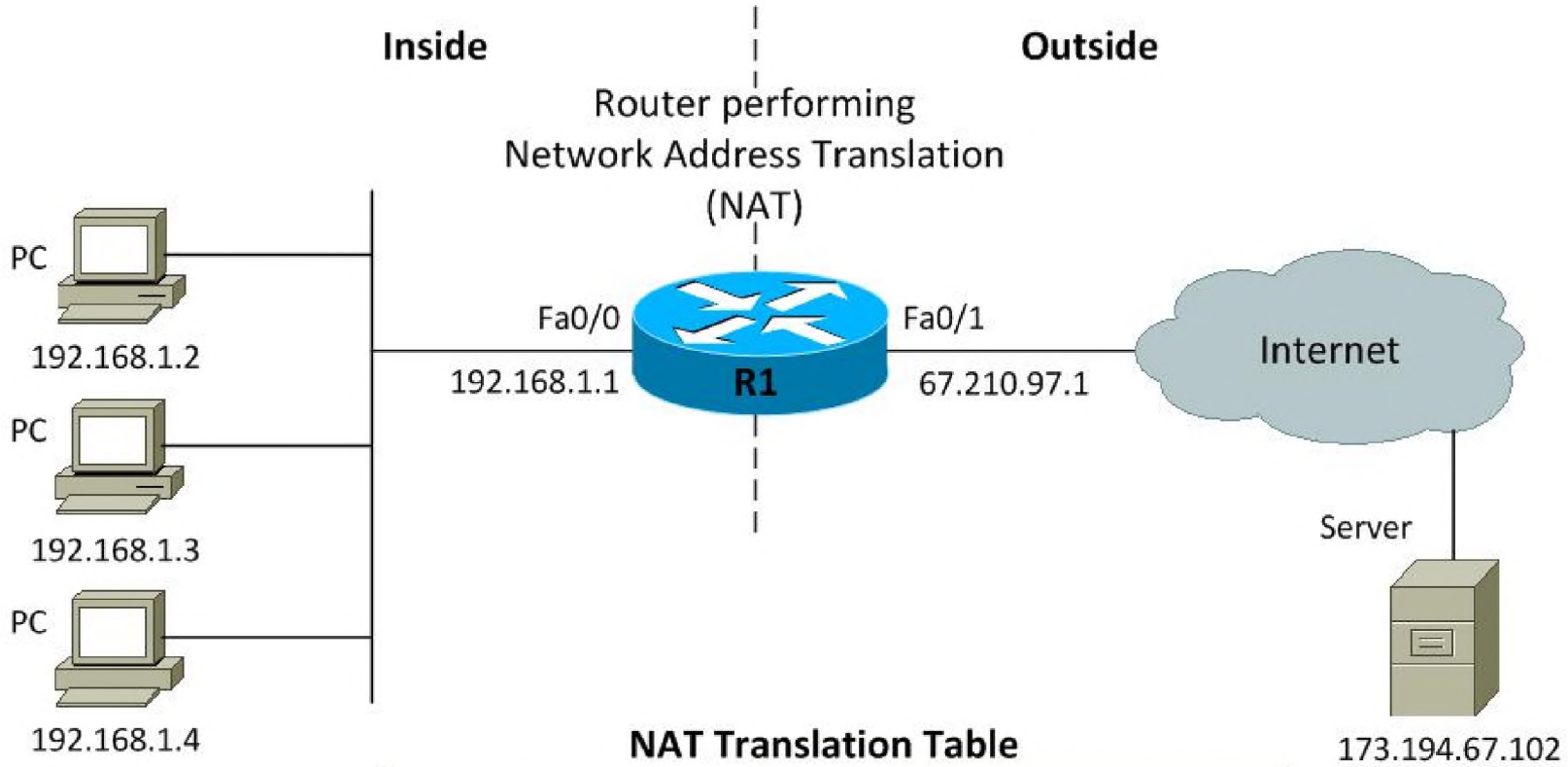
15. NAT (Network Address Translation - Ağ Adresi Çeviricisi)

- Temel olarak bir NAT yönlendiricisi, NAT tablosu adı verilen bir tablo yardımıyla IP çevirme işlemini gerçekleştirir. Kullanıcının bilgisayarında özel IP adresleri aralığından bir adres bulunur. Buradan yerel ağın içinde olmayan bir adrese gitmek için bir talep gelince, NAT yönlendiricisi daha önceden kullanıcının ayarladığı NAT tablosuna bakarak, özel IP adresini genel bir IP adresine çevirir ve bu şekilde dış ağlara ya da İnternete çıkılmış olur. Yönlendiricinin çeviri yaparak değiştirdiği bu IP, kullanıcının İnternetteki bilinen IP'sidir. Aynı şekilde dış ağlardan bu bilinen IP'ye doğru bir istek gelince, yönlendirici tablosuna bakarak bu IP'yi kullanıcın özel IP adresine yönlendirir ve paketi kullanıcının bilgisayarına gönderir

15. NAT (Network Address Translation - Ağ Adresi Çeviricisi)

- **İç Yerel Adres:** NAT tarafından özel IP adresleri aralığı içerisinden kullanıcıya yerel ağda kullanması için atanmış şekildeki 192.168.2.1 gibi bir adrestir.
- **İç Global Adres:** NAT'ın dış ağlara bakan yüzünde bulunan ve dış ağlara bağlanırken kullanılan genel IP adresleri aralığından şekildeki 160.75.67.67 gibi bir adrestir.
- **Dış Global Adres:** İnternette bulunan herhangi bir kullanıcının veya sunucunun sahip olduğu genel IP adresleri aralığından herhangi bir adrestir.

Network Address Translation



NAT Translation Table

Protocol	Inside Local IP : Port	Inside Global IP : Port
ICMP	192.168.1.2 : 18	67.210.97.1 : 18
ICMP	192.168.1.3 : 19	67.210.97.1 : 19
ICMP	192.168.1.4 : 20	67.210.97.1 : 20

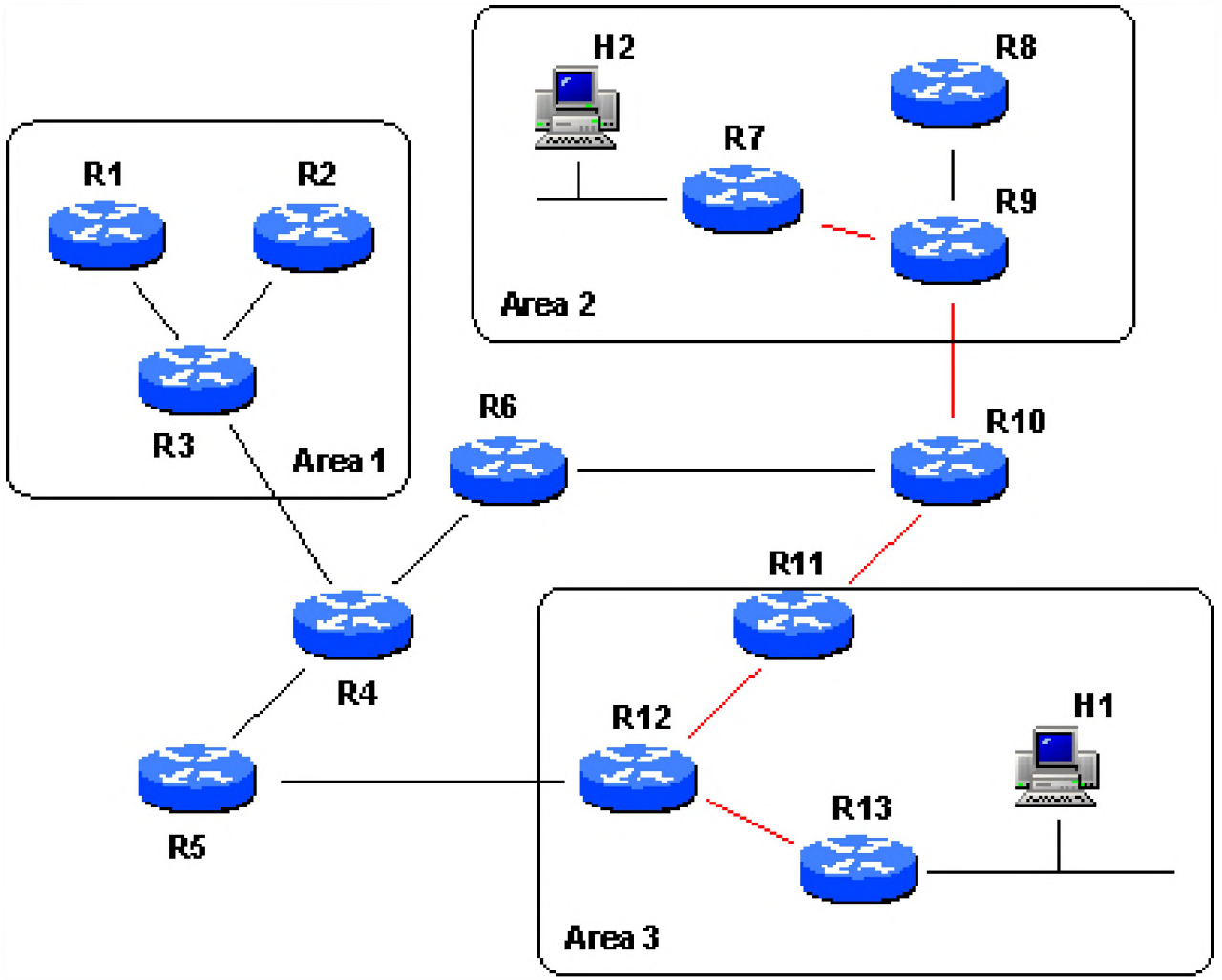
16. OSPF (Open Shortest Path First - Önce Açık En Kısa Yol) Protokolü

- OSPF, RIP'te bulunan bazı eksik yanları geliştirmek ve düzeltmek için IETF (Internet Engineering Task Force – İnternet Mühendisliği Görev Gücü) tarafından geliştirilmiş bir protokoldür.
- RIP (Routing Information Protocol - Yönlendirme Bilgi Protokolü)'ın aksine OSPF "link state" (Hat Durumu) protokolü olarak tasarlanmıştır. Bu protokollerle çalışan yönlendiriciler, diğer yönlendiricilerden öğrendikleri bilgileri kullanarak, tüm ağın topoloji haritasını çıkarabilirler.
- Buna göre yönlendiriciler ağdaki iki nokta arasında bulunan tüm yolların bilgisine ulaştıktan sonra SPF (Shortest Path First -Önce En Kısa Yol) algoritmalarını kullanarak hangi yolun en iyisi olduğuna karar verirler.

16. OSPF (Open Shortest Path First - Önce Açık En Kısa Yol) Protokolü

- OSPF protokolünü diğer protokollerden farklı yapan en önemli avantajı hat durumu protokolü olmasıdır. Buna göre OSPF, RIP'ten farklı olarak yol bilgisini hızlı bir şekilde öğrenme, büyük ve karmaşık ağlarda daha iyi çalışabilme ve güvenilirlik konularında oldukça başarılıdır.
- Bu protokole göre, yönlendiriciler içinde bulunduğu ağı öğrenebilmek için 10 saniye aralıklara "multicast" (Gruba özel) "Hello" paketleri gönderir ve bu paketlerin içerisinde bulunan Alan ID, Kimlik Doğrulama, Ağ Maskesi gibi çeşitli değerlerin aynı olup olmamasına bakılarak yönlendiricilerin komşu olup olmadığına karar verilir.

Open Shortest Path First



17. SNMP (Simple Network Management Protocol - Basit Ağ Yönetim Protokolü)

- Ağı yönetirken, ağ yöneticisine yardımcı olan basit bir uygulama katmanı protokolüdür. Temel anlamda, geniş ağlarda cihazların yönetimini ve denetimini kolaylaştırmak için tasarlanmıştır.
- SNMP kullanılarak ağda bulunan Yönlendirici (Router), Anahtarlayıcı (Switch), Erişim Sunucusu (Access Server), Köprü (Bridge) ve hatta bilgisayar gibi cihazların sıcaklık, cihaza bağlı kullanıcılar, İnternet bağlantı hızı, cihaz çalışma süresi gibi temel bilgiler elde edilebilir.
- TCP/IP protokolünün bir parçası olan SNMP, IP adreslerini kullandığı için sadece kendi fiziksel ağını değil yönlendiricilerin diğer arayüzlerinin de kontrol edilmesini sağlar.
- SNMP, ajan uygulama, yönetici uygulama ve ağ yönetim sistemi adı verilen 3 bileşenden oluşmaktadır.

17. SNMP (Simple Network Management Protocol - Basit Ağ Yönetim Protokolü)

- **Ajan Uygulama:** Ağdaki cihazlar üzerinde çalışan uygulamadır. Bu uygulama ile cihazın gerekli bilgileri alınır ve kayıtlı tutularak yönetici uygulamaya aktarılır. Aynı şekilde yöneticiden gelen değişiklikler bu uygulama tarafından cihaza uygulanır. Yani kısacası bu uygulama, SNMP'nin, kullanılacağı cihazlar üzerinde çalışan bileşenidir.
- **Yönetici Uygulama:** Ajan uygulama ile ağ yöneticisi arasındaki bilgi akışını sağlayan uygulamadır. Yani, ajan uygulamadan aldığı cihaz bilgilerini yöneticiye, yöneticiden aldığı yapılandırma değişiklik isteklerini de ajan uygulamaya ileten bileşendir.
- **Ağ Yönetim Sistemi:** Yönetici birimde çalışan ve tüm ağdaki cihazların bilgilerinin eş zamanlı olarak izlenmesini ve yönetimini sağlayan yazılımdır.

Simple Network Management Protocol