Network Throubleshooting

Bu bölümün misyonu networkte oluşan problemlerin giderilme sürecinde neler yapılabileceğini açıklamaya çalışmaktır. Oluşan bir problemin çözüm sürecinde;

- Network için tutulan dökümantasyonlar incelenmelidir. Bu sayede topolojide kaç cihaz olduğu, fiziksel ve mantıksal topolojiler, cihazların konum bilgileri, seri numaraları, MAC adresleri gibi çeşitli konularda fikir sahibi olmak problemi anlamaya yardımcı olacaktır.
- Networkte oluşan sorunun ne zamandan beri olduğu ve bu süre içerisinde ne gibi değişikliklerin yapıldığı öğrenilmeli.
- Oluşan problemin kapsamı öğrenilmeli ve bu doğrultuda Throubleshooting yapılmaya başlanmalı.

Çözüm Sürecinde;

- Problem tarif edilir
- Problemle ilgili bilgiler toplanır
- Bilgilerin analiz edilir
- Problem olması muhtemel noktaların belirlenir
- Belirlenen noktaların test edilir ve problem varsa düzeltilir
- Yaşanan genel problemin çözülüp çözülmediği kontrol edilir.

Network İçin Dökümantasyon Oluşturulurken;

- İlk olarak topolojide kullanılan cihazlar için hangi bilgilerin tutulacağı/tutulması gerektiği belirlenmeli.
- Topoloji haritası oluşturulmalı. Topoloji haritası oluşturulurken CDP veya LLDP gibi protokoller kullanılabiliyor (İstemcilerin de bilgisi tutulmak isteniyorsa switchler üzerindeki ARP tablosu kullanılabiliyor). Bunun için hazırlanmış yazılımlar da mevcuttur.
- **Network Baseline** oluşturulmalı. Bunun için en az 2-4 hafta network trafiğinin monitor edilmesi gerekiyor. Bu sayede anomali tespiti yapılabiliyor.

Son Kullanıcıya Sorulabilecek Sorular

- Problemin ne olduğuyla ilgili sorular sorulmalı.
    - Neyin çalışmadığı?, Nereye erişilemediği? gibi sorular.
- Problemin kapsamını belirlemek üzerine sorular sorulmalı.
    - Problemin sadece kendinde mi yoksa diğer kullanıcılarda da mı olduğu?
    - Hangi cihazlarda yaşandığı (cihaz bazlı sorular)?
- Oluşan problemi belirlemek üzerine sorular sorulmalı.
    - Herhangi bir hata mesajı alındı mı?
- Problemin sürekli mi yoksa belirli aralıklarla mı yaşandığı sorulmalı.
    - Mümkünse problemle ilgili video veya ekran görüntüsü istenebilir.
- Problem öncesinde herhangi bir değişiklik yapılıp yapılmadığı sorulmalı.

Bağlantı Testi Gerçekleştirilirken Kullanılan Komutlar;

- **ping**, iki cihaz arasında bağlantı testi için kullanılıyor.
- **traceroute**, kullanılan rota üzerinde bir problem olup olmadığını kontrol çin kullanılıyor.
- **telnet**, Telnet farklı portlara atanabiliyor. Bu sayede farklı portların doğru çalışıp çalışmadığını test edilebiliyor.
- **Ssh –l**, cihaza erişimi kontrol etmek için kullanılıyor.
- **sh ip int brief**, arayüzün durumu hakkında bilgi toplamak için kullanılıyor.
- **sh ip route**, yönledirme tablosunu kontrol etmek için kullanılıyor.
- **sh protocols**, L3 protokollerinin hangilerinin kullanıldığını görüntülemek için kullanılıyor.
- **debug**, gerçek zamanlı takip edilmek istenen özelliklerde gerçekleştirilen değişimlerin takip edilebilmesi için kullanılıyor.

Problem Çözme Yaklaşımları;

- **Bottom-Up**, ISO modelinin en alt seviyesinden (L1 -> L7) başlayarak üst seviyesine doğru kontrol etme yaklaşımıdır.
- **Top-Down**, OSI modelinin en üst seviyesinden (L7 -> L1) başlayarak en alt seviyesine doğru kontrol etme yaklaşımıdır.
- **Divide-and-Conquer**, orta katmandan (L3) başlayarak duruma göre üst veya alt katmanlara doğru ilerleyerek problemi çözme yaklaşımıdır.
- **Follow-the-Path**, hedef ve kaynak arasındaki tüm cihazlara tek tek bağlanılarak Throubleshooting yapılmasıyla problemin çözülmesini sağlayan yaklaşımdır.
- **Subsitution**, networkte fiziksel bir problem yaşandığında problem olması muhtemel bir cihaz yerine çalışan bir tane yerleştirilerek sorunu tespit edip çözülmesini sağlayan yaklaşımdır (Cihaz sadece açıklama için kullanılan bir örnek. Burada kabloların bağlı olduğu portları değiştirilmesi de örnek olarak verilebilir).
- **Comparison**, çalışan bir cihazla problem yaşanan cihaz karşılaştırılarak farklılıkları üzerinden problemleri tespit edip gidermesinin sağlandığı bir yaklaşımdır.
- **Educated Guess**, daha önce yaşanmış problemler göz önünde bulundurularak problemin kaynağının tespit edilip, giderilmesini sağlayan yaklaşımdır.

Sorun Giderme Konusunda Kullanılabilecek Araçlar/Yazılımlar

- Networkü monitor edebilmek için kullanılan araçlar (Network Management System Tools).
- Daha önce yaşanmış problemlerde kullanılan çözümlerin not edildiği kaynaklar (kurumun tuttuğu dökümanlar veya internet üzerindek aynı cihazı kullanan kişilerin paylaştığı case'ler, forumlar gibi).
- Kullanılan Network Baseline yazılımları.
- Cihazlarda gerçekleşen değişimleirn kaydedildiği loglar / Syslog sunucuları.

L1'de Ouşabilecek Problemlerin Tespitinde Kullanılan Donanımsal Araclar

- Digital Multimeters
- Cable Testers, kablolamada yaşanan problemleri/kopuklukları tespit etmek için kullanılıyor.
- Cable Analyzers, kablonun düzgü sonlandırılıp sonlandırılmaığını / sinyal kayıplarını (özetle kaliteyi) ölçmek için kullanılan cihazlar olarak tanımlanabilir.
- Portable Network Analyzers, network analizi için kullanılan küçük ve taşınabilir cihazlar olarak tanımlanabilir.

L1 İle İlgili Bir Problem Oluştuğunda Görülebilecek Tepkiler

- Network performansında düşüş görülebilir (Baseline'da düşüş görülecektir).
- Bağlantı kesilmeleri oluşabilir.
- Networkte tıkanıklıklar oluşabilir.
- Cihazların CPU kullanımında artışlar gözlemlenebilir.
- Konsol ekranlarında veya Syslog sunucularında daha önce karşılaşılmamış/farklı hata mesajları görülmeye başlanabilir.

L1'de Oluşabilecek Olası Problemler

- Cihazların güç sağlayıcılarından kaynaklı problemler görülebilir.
- Cihazların NIC kartı gibi çeşitli donanımsal arızalardan kaynaklanıyor olabilir.
- Kullanılan kablolarda kopmalar, yanlış sonlandırmalar gibi nedenlerden kaynaklanıyor olabilir.
- Çevre etmenlerden/gürültülerden kaynaklanıyor olabilir (Elektromanyetik dalgalanamlardan vs).
- Uzun kablolamalarda sinyal zayflamalarından kaynaklanıyor olabilir.
- Cihazın CPU'suna fazla yüklenilmiş olabilir.

L2 İle İlgili Bir Problem Oluştuğunda Görülebilecek Tepkiler

- Cihazdan ping atılamıyor (L3 çalışmıyor) ama L1'de bağlantı görünebilir.
- Normalden daha fazla Broascast paketleri görülüyorsa bir Loop oluşmuş olabilir.
    - Networkte kamera kullanılıyorsa Multicast kullanımı araştırılmalı. Aksi taktirde kameralar Broadcast kullanacak ve bu durumda oluşturulan bütün Broadcast pakleri networkteki diğer cihazları olumsuz etkileyecektir.
- Yanlış konfigürasyonlardan kaynaklı network performansı düşebilir.
    - Örnek olarak STP protokolüyle Root Bridge seçiminden kaynaklı düşük bant genişliğine sahip bağantılar bloklanabilir. Bu durumda trafik daha düşük bant genişliklerinden geçirilecek ve dar boğaza neden olacaktır.

L2'de Oluşabilecek Olası Problemler

- Karşılıklı cihazlarda farklı protokoller kullanıldığında Encapsulation hatalarıyla karşılaılabilir.
- ARP tablosuna girilmiş statik bir kayıt veya Port-Security özelliğiyle tanımlanmış belirli MAC adresleri gibi çeştli konfigürasyonlardan kaynaklı hatalarla karşılaşılabilir.
- Framlerde oluşan hatalarla karşılaşılabilir.
- STP protokolünden kaynaklı loop oluşumlarıyla karşılşılabilir.

L3 İle İlgili Bir Problem Oluştuğunda Görülebilecek Tepkiler

- Erişimde kesintiler veya yavaşlamalar meydana gelebilir.

L3'de Oluşabilecek Olası Problemler

- Topoloji değişimiş olabilir (Yönlendirme tablolarında değişimler olabilir).
- ISP tarafında yaşanan problemler olabilir.
- Arayüze uygulanan ACL'lerden kaynaklanan problem olabilir.
- Yönlendirme tablolarından kaynaklı hatalar oluşabilir.
    - Dinamik yönlendirme protokollerinde komşuluk kurulmamış olabilir.
    - Topology Database üzerinde oluşan hata kaynaklı yönlendirme tablolarında problem oluşuyor olabilir.

L4'de Oluşabilecek Olası Problemler

- Yanlış tanımlanmış ACE'şer veya yanlış arayüze yanlış yönde uygulanmış ACL'lerden kaynaklı hatalar oluşabilir.
    - ACL'lerde ACE'lerin tanımlanma sırasından kaynaklı da olabilir.
    - Tanımlamalarda Wildcard maskesi yerine Subnet maskesi kullanılmış olabilir.
- ACL'lerde Implicit Deny satırı unutulmuş olabilir.
- Extended ACL tanımlamalarında tanımlanan protocol tipi yanlış tanımlanmış olabilir.
    - Portların numaraları yanlış tanımlanmış olabilir.
- "Established" kelimesi doğru kullanılmamış olabilir.
- ACE tanımlanırken kullanılan protokol ismi algılanmıyor olabilir.
    - Bu durumda protocol numarasıyla tarif edilmesi gerekiyor.

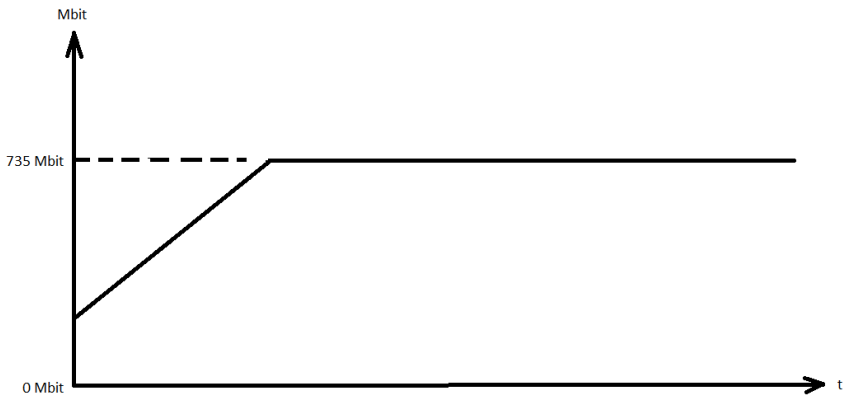
NAT Protokolüyle İlgili Oluşabilecek Problemler

- Networkün DHCP sunucusu uzak bir lokasyonda olabilir. Bu durumda "**ip helper-address <DHCP Server İp Address>**" komutu kullanılmamış olabilir (Bu sayede router kaynak ip adresini değiştirerek paketi Unicast şekilde DHCP sunucusuna gönderebiliyor) veya routerda uzak DHCP sunucusu unutularak engellemeler (ACL'ler) tanımlanmış olabilir.
    - Bu türden ACL'ler tanımlanırken altyapıda kullanılan protokollerin engellenmediğinden emin olmak gerekiyor. Örnek olarak OSPF protokolünün kullandığı paketler yanlışlıkla engellenirse hiçbir dinamik rota öğrenilemez.

- Network içerisinde tanımlanmış bir local sunucu Port-Forwarding yapılarak (burada routerun public ip adresi kullanılıyor – sunucunun “mfi.com” alan adına sahip olduğunu varsayalım) internet üzerindeki bir DNS sunucusuna keydedildiğinde (yine routerun dış bacağındaki public ip adresiyle kaydoluyor) aynı networke dahil bir istemci localde kullanılan sunucuya erişemeyecektir. Nedeni aynı localde bulunan istemci internet üzerindeki DNS sunucusuna localde bulunan sunucunun alan adını (mfi.com) sorduğunda DNS sunucusundan yanıt olarak kendiyle aynı adrese sahip bir ip adresi alacak olmasıdır. Bu duruma çözüm olarak;
    - End-point’lere tek tek statik domain-ip eşleniği tanımlanabilir.
    - Local network dışına ikinci bir kopya sunucu daha yerleştirmek olacaktır. Bu sayede sunucu farklı bir ip adresine sahip olacağı için localdeki istemciler sorunsuzca erişebilecektir.
    - Local networke ikinci bir server kurularak farklı Public Ip adresiyle NAT yapılması sağlanabilir.
- VPN gibi tünelleme ve şifreleme protokollerinde kaynak ve hedef ip adresi Private ip adresleri olduğu için **NAT konfigürasyonlarında adres dönüşümü engellenmediği durumlarda** Private ip adresler internete çıkarılırken NAT’a tabi tutulacaktır. Kaynak ip adres Public ip adresine dönüşeceği için hedef networke gönderilen paketlerden dönüş alınamayacaktır. Yani tünelleme protokolü çalışmadığı durumlarda NAT konfigürasyonunda tünelleme yapılacak Private ip adresler için engelleme kuralı yazılmamış olabilir.

NOT

- İnternete çıkış için bant genişliği yetersiz kaldığı durumda NMS yazılımında aşağıdakai gibi bir görsel görünecektir. Bu görselde trafiğin düz olması belirli bant genişliğinden yüksek gelen trafiğin Drop edildiğini gösterir. Bu durumda;
    - Bant genişliğinin gereksiz kullanılıp kullanılmadığı araştırılarak gereksiz kullanımlar engellenmeli.
    - Gereksiz kullanım yoksa ISP’den daha yüksek bant genişliği alınmalı.



- Problemin çözüm sürecinden end-user’a asla güvenme :D.
- Gece saatlarinden gerçekleşen problemlerde saat veya tarihle ilgili değişimlerden kaynaklı problemler yaşanıyor olabilir (Kullanılan lisansların süresi bitmiş olabilir).
- NAT arkasında bulunan bir SNMP sunucusuyla yine NAT arkasında bulunan bir SNMP Agent’ın haberleştirilmesi istendiği durumda VPN gibi tünelleme protokolleri kullanılabiliyor.

Terminolojiler

- Fiziksel topoloji, networkün fiziksel olarak nasıl oluştuğunu gösteren topolojidir. Mantıksal Topoloji, networkteki veri akışının nasıl gerçekleştirğini gösteren topololojidir.
- Network Baseline, network performansını ölçmek için kullanılan bir yöntemdir. Networkün gün içerisinde oluşturduğu trafik temel alınıyor. Bu sayede networkte bir anomali oluştuğunda Nsetwork Baseline temel alınarak anomali tespiti yapılabiliyor.
- Mirrior/Span Port, switch portlarından birine switch üzerinden geçen paketlerin bir kopyasının gönderildiği portlara verilen isimdir. Bu sayede bu porta bir cihaz bağlanarak switch üzerinden geçen bütün trafik görüntülenebilmektedir. Bu port kullanılarak birçok switch üzerinden gecen trafik farklı bir network üzerindeki cihaza gönderilerek izlenebilmektedir (RSPAN).
    - Switch üzerinden gecen trafiğin bant genişliğinin dinlenecek portun bant genişliğinden küçük veya eşit olması gerkeiyor. Aksi taktirde bütün trafik dinlenemez (Mirrior/Span portun bant genişliğinden büyük trafik Drop edilir).

Kontrol Komutları

- sh version
- sh ip int brief
- sh interfaces
- sh ip route [static|eigrp|ospf|bgp]
- sh cdp neighbors detail
- sh arp
- sh run
- sh vlan
- sh port
- sh tech-support
- sh proc cpu