ŞARTNAME

Kenar Anahtar (5-adet)

1. Anahtar üzerinde en az 48 adet 10/100/1000BaseT ethernet portu ve en az 2 adet SFP + tabanlı yuva bulunmalıdır. Bu yuvalara 1000BASE-LX/LH, 1000BASE-SX, 1000BASE-BX, 1000BASE-ZX, SFP-10G-LR, SFP-10G-SR, SFP-10G-LRM, SFP-10G-ER fiber arayüzleri takılabilmelidir. 50 port aynı anda aktif olarak çalışmalıdır.
2. Dönüştürücü ile anahtar aynı üretici tarafından üretilmelidir ve 10GBASE-SR standardında olmalıdır.
3. Anahtarın tüm portları tıkanmasız ve line-rate çalışmalıdır.
4. Anahtarlama bant genişliği en az 216 Gbps olmalıdır.
5. Anahtarın 64-Byte'lık L3 paketlerinde en az L2 anahtarlama performans değeri en az 130 Mpps olmalıdır.
6. En az 16,000 adet unicast MAC adresi desteklenmelidir.
7. En az 512MB DRAM'e sahip olmalıdır.
8. En az 128MB Flash belleği olmalıdır.
9. Cihazın MTBF (mean time between failure) değeri 230.000 saatten daha az olmayacak ve açıkca belirtilecektir.
10. Tüm portlar üzerinde IEEE 802.1Q VLAN trunking protokolü desteklenmelidir. Cihazın desteklediği VLAN ID sayısı en az 4000, aktif VLAN sayısı en az 1000 olmalıdır. Port bazında VLAN tanımlanabilmelidir.
11. Cihaz üzerinde en az 8 adet 10/100/1000Base T port ayrı ayrı kanal altında toplanıp, tek port gibi çalışabilmelidir. En az 24 adet kanal (Port-Channel) tanımlanabilmelidir. IEEE 802.3ad standardı desteklenmelidir.
12. Bütün 10/100/1000BaseT portlar hem half-duplex hem de full-duplex çalışabilir olmalıdır. Port hızları otomatik olarak algılanabilmelidir. IEEE 802.3x standardı desteklenmelidir.
13. Cihazın "QoS (Quality of Service)" desteği bulunmalıdır. Üçüncü seviyede (L3) DiffServ Code Point (DSCP) ya da ikinci seviyede (L2) IEEE 802.1p CoS (Class of Service) ile sınıflandırılmış paketlerin öncelik değerlerini anlayabilmeli, gerektiğinde bu öncelik değerlerini değiştirebilmelidir. Paketleri, ayrıca L2 başlığındaki kaynak/hedef MAC adresi, L3 başlığındaki kaynak/hedef IP adresi, L4 başlığındaki TCP/UDP port numarası bilgilerine göre sınıflandırabilmelidir. Cihaz üzerindeki her portun en az 4 adet kuyruğu bulunmalıdır.
14. Anahtarın her 10/100/1000 bakır portunda auto-MDIX (automatic medium-dependent interface crossover) özelliği bulunmalıdır.
15. Anahtar üzerinde, her porta ait durum/duplex/hız bilgisi veren LED'ler bulunmalıdır.
16. IEEE 802.3, 802.3u, 802.3ab standartlarını desteklenmelidir.
17. Anahtar, gerektiğinde harici bir güç kaynağı takılarak, güç kaynağı yedeklemesine sahip olabilmelidir.
18. Anahtar, TDR (Time Domain Reflector) özelliğini yada wire inspection özelliğini destekleyecektir.
19. Anahtar, jumbo frame desteğine sahip olmalıdır. Desteklenen jumbo frame'lerin uzunluğu, en az 9216 byte olmalıdır.
20. Fiber kablolardaki arızalar nedeniyle oluşabilecek tek yönlü trafik problemlerini belirleyip ilgili portu kullanım dışı bırakarak, olası bir loop oluşmasını engelleyebilmelidir (*UDLD yada benzer bir protokol*)
21. Anahtar 802.3af ve 802.3at standartlarını desteklemelidir.
22. Anahtar 48 portundan 15,4 ve en az 24 portundan 30W güç sağlayabilmelidir.
23. Anahtar yığınlanabilir (stackable) yapıda olmalı veya istenmesi halinde yığınlanabilir hale getirilebilmelidir. Yığınlama için özel yığınlama portları kullanılmalı, kullanıcı veya uplink portları kullanılmamalıdır. Anahtar üzerinde 2 adet yığınlama arayüzü bulunmalı veya istenmesi halinde ayrıca eklenebilmelidir.
24. En az 8 adet anahtar tek bir yığın içinde bulunabilmelidir.
25. Yığınlama yapılması halinde, yığındaki anahtarlar arasındaki band genişliği en az 40 Gbps olmalıdır.
26. Yığınlama yapılması halinde yığın içindeki anahtarlardan birisinin arızalanması durumunda, yığın içindeki diğer anahtarlar çalışmaya devam edebilmelidir.
27. Yığın tek bir IP adresi üzerinden yönetilebilmeli, yığındaki anahtarların ayrı ayrı yönetilmesi gerekmemelidir.
28. Yığın içindeki farklı anahtarlara ait portlar tek bir kanal altında toplanabilmelidir. *(Cross-stack Etherchannel)*
29. Yığına yeni bir anahtar eklendiğinde otomatik olarak yazılımı güncellenmeli ve herhangi bir konfigürasyon yapılmadan yığının bir üyesi olabilmelidir.
30. En az 0.5m, 1m ve 3m boyutlarında yığınlama kablosu çeşitliliğine sahip olmalıdır.
31. Anahtar, IEEE 802.1d, 802.1w ve 802.1s "spanning tree" protokollerini desteklemelidir.
32. Anahtar üzerinde her VLAN için farklı "spanning tree" kullanılabilmelidir.
33. Anahtar, kullanıcı ve trunk portlarında spanning tree hesaplarını hızlandırabilmelidir. (*Port-fast*)
34. Anahtarın BPDU (Bridge Protocol Data Unit) Guard özelliği bulunacaktır. Bu sayede Spanning Tree grubunda olmayan portlara, o grubun BPDU paketlerinin girişi engellenecektir.
35. Anahtarın Spanning Tree Root Guard (STRG) özelliği bulunacaktır. Bu sayede network yöneticisinin kontrolünde olmayan anahtarların, Spanning Tree protokolü için root anahtar olması engellenebilecektir.

Yücel KAPLAN
Bilgi İşlem Teknik Donanım
Birim Sorumlusu

36. Anahtar statik routing yapabilmelidir. Anahtar üzerinde en az 16 adet statik route tanımlanabilmelidir.
37. Cihaz, erişim kontrol listeleri ile paketleri L2 başlığındaki kaynak/hedef MAC adresi, L3 başlığındaki kaynak/hedef IP adresi, L4 başlığındaki TCP/UDP port numarası bilgilerine göre erişim denetiminden geçirebilmelidir. Cihaz Erişim Kotrol Listeleri direk olarak L2 veya L3 porta ugulanabileceği gibi VLAN içindeki trafiği de filtreleyebilmelidir. (*Router ACL, VLAN ACL, Port-Based ACL)*
38. Anahtar üzerinde bulunan her port için MAC adresi bazında kullanıcı listeleri oluşturulabilmeli ve böylece port güvenliği sağlanabilmelidir. (*Port-Security*)
39. Anahtar, MAC adresi tablosuna yeni bir adres eklendiğinde, ya da bu tablodan bir adres silindiğinde, bu durumu SNMP yönetim sunucusuna raporlamalıdır. (*MAC Address Notification*)
40. Anahtarın IEEE 802.1x desteği bulunacak ve aşağıda belirtilen 802.1x özellikleri desteklenecektir.
    a. 802.1x VLAN assignment; Radius server yardımı ile port bazında kullanıcı yetkilendirme ve dinamik VLAN tahsisi
    b. 802.1x Port Security; Port security özelliği, 802.1x etkin bir port üzerinde tanımlanabilmelidir.
    c. 802.1x Guest VLAN
    d. 802.1x Web yetkilendirmesi
41. Anahtar, IEEE 802.1x protokolünü kullanarak, radius server yardımı ile port bazında kullanıcı yetkilendirme desteklemelidir. Anahtar, Radius tarafından gönderilen yetkilendirme değişiklik taleplerini yerine getirebilmeilidir. *(Change of Authorization)*
42. Anahtarın 802.1X MAC authentication bypass özelliği bulunacaktır.
43. Anahtar aynı port üzerindeki birden farklı domain'deki cihazların kimlik doğrulama işlemlerini yapabilecektir. Böylece aynı porttaki bir PC ile IP Telefonun ayrı ayrı kimlikleri doğrulayıp uygun veri ve ses VLAN'ilerine atamalarını yapabilecektir. (*Multi-Domain Authentication*)
44. IP Spoofing ataklarının engellenebilmesi için, otomatik olarak anahtarın belirtilen portlarına kaynak IP address filtreleri yazılabilecektir (*IP Source Guard*).
45. Anahtarın Dynamic ARP Inspection (DAI) özelliği bulunacaktır. Anahtar, üzerinden geçen tüm ARP istek ve cevaplarını incelemeli ve her ARP paketi, IP-MAC binding tablosu ile eşleştirebilmelidir. Eşleşmeyen paketler drop edilebilmelidir.
46. Anahtarın multicast desteği olmalıdır. IGMP filtering, ve IGMP Snooping v1-v2-v3, IPv6 MLD v1-v2 snooping desteklenmelidir.
47. Anahtar, en az 256 adet IGMP grubu desteklemelidir.
48. Anahtar, IGMP snooping timer, IGMP throttle, IGMP querier ve Configurable IGMP leave timer özelliklerini desteklemelidir.
49. Portlardaki trafik yoğunlukları arasındaki sessiz anları belirleyerek, bu zaman aralıklarında portların daha az güç tüketmesini sağlayabilmelidir. (*Energy Efficient Ethernet*)
50. Anahtar, gece veya haftasonu gibi kullanılmadığı zaman aralıklarında çok düşük güç tüketeceği uyku modunu desteklemelidir. Bu işlem için 'EnergyWise' uyumlu yazılımlar ile uyumlu çalışabilmelidir. (Switch Hibernation Mode)
51. Anahtar, SNMP v1, v2, v3, telnet, Secure Shell (SSH), SSL, SCP (Secure Copy Protocol), HTTP (web) ve konsol aracılığı ile yönetilebilmeli veya gözlenebilmelidir.
52. Anahtarı yönetmek isteyen kişiler Radius sorgulama protokolü tarafından sorgulanabilmelidirler.
53. TFTP yardımı ile işletim sistemi güncellemesi yapılabilmelidir.
54. Cihazın tüm portları en az 4 adet RMON grubunu (history, statistics, alarms, events) desteklemelidir.
55. Detaylı gerçek zamanlı trafik analizi yapabilmek için port mirroring desteği bulunmalıdır. Birden fazla kaynak portu, hedef portuna aynalanabilmelidir. Aynı anda en az 4 adet port mirroring tanımlanabilmelidir.
56. Anahtarın saat ve tarih bilgisi, ağ üzerindeki diğer tüm anahtarlarla senkron hale getirilebilecektir

Yücel KAPLAN
Bilgi İşlem Teknik Donanım
Birim Sorumlusu