**Bu şartname genel bir şartname olup markaya özel değildir.**

**OMURGA ANAHTAR**

* + 1. Omurga anahtarlar ile kenar anahtarlar aynı marka olacaktır.
    2. Teklif edilecek omurga anahtarlar en az 18 slotlu ve şasi tipinde olacaktır.
    3. Cihazın yönetim modülü yedeklenmelidir.
    4. IEEE 802.3 (10BaseT Ethernet), 802.3u (100BaseT), 802.3z (1000BaseX), 802.3ab (1000BaseT) standartlarını desteklemeli ve anahtarın slotları 100BaseFX, 10/100/1000 BaseT, 1000BaseSX, 1000BaseLX, 1000BaseBX, 10GBase-SR, 10GBase-LR ve 10Gbase-ER portlar ile doldurulabilmelidir.
    5. Teklif edilecek omurga anahtar, 100 (yüz) BaseFX bağlantılarını, çevirici (media converter) kullanılmadan desteklemelidir. Anahtar en az 168 adet 100BaseFX port desteklemelidir.
    6. Teklif edilecek omurga anahtar en az 384 adet 10/100/1000BaseT port desteklemelidir.
    7. Teklif edilecek omurga anahtar en az 384 adet 1000 (Bin) BaseX port desteklemelidir.
    8. Teklif edilecek omurga anahtar üzerinde ………………… 10/100/1000BaseT port bulunacaktır.
    9. Teklif edilecek omurga anahtar en az 384 adet 10 Gigabitport desteklemelidir.
    10. Teklif edilecek omurga anahtar üzerinde en az ………..adet 1000 (Bin) BaseX port bulunacaktır. Anahtar, 1000 (Bin) BaseX bağlantılarını, çevirici (media converter) kullanılmadan desteklemelidir. Bu portlar için …….1000BaseLX SFP/GBIC modül teklif edilecektir.
    11. Fiber ve bakır portlar aynı modüller üzerinde bulunmamalı ve ayrı modüller üzerinde teklif edilmelidir.
    12. Anahtar üzerinde teklif edilen tüm ara yüz kartları ve ara yüzler anahtar üreticisi tarafından üretilen orijinal ürünler olmalıdır.
    13. Teklif edilecek omurga anahtarın backplane bantgenişliği en az 3.0 tbps Switching kapasitesi en az 1.5Tbps olmalıdır. Anahtarın L2 anahtarlama ve L3 yönlendirme performans değeri, şasi dolu durumda iken 950 Mpps’a kadar ölçeklenebilmelidir.
    14. Anahtarın üzerindeki I/O modülleri, Fabric Modüllerinden bağımsız olarak teklif edilecektir. Fabric modüller üzerinde teklif edilen portlar , ihtiyaç duyulan port sayılarına dahil edilmeyecektir.
    15. Anahtar Distributed Forwarding (DFC)yapısına sahip olacak,her I/O modülü kendi yönlendirmesini yapabilecektir.I/O Modüller arasındaki bant genişliği en

az 40 Gbps olacaktır.

* + 1. Anahtar üzerinde teklif edilecek 10 gigabit, 1000BaseX ve 10/100/1000Base-T kartlar birbirinden bağımsız olarak backplane bağlantısına sahip olmalıdır.
    2. Teklif edilecek omurga anahtar üreticinin yayınlamış olduğu en yüksek performanslı (memory, bellek ve özellik) donanım ile teklif edilecektir. Alt versiyonlar kesinlikle teklif edilmemelidir.
    3. Omurga anahtarın, tüm slotları dolu durumda iken güç kaynağı yedeklemesine sahip olmalıdır. Bir güç kaynağının arızalanması durumunda anahtar üzerinde hiç bir modül devre dışı kalmayacaktır.Cihazla birlikte yedek güç kaynağı verilmelidir.
    4. Omurga anahtar üzerindeki tüm I/O modüller, güç kaynakları, GBIC/SFP optikler, XENPAK/XFP/X2/SFP+ optikler cihaz çalışırken çıkarılıp takılabilmelidirler (hot-swappable olmalıdırlar).
    5. Teklif edilecek omurga anahtar, en az 2.000.000 adet MAC adresi destekleyecektir.
    6. Tüm portlar üzerinde IEEE 802.1Q VLAN trunking protokolü desteklenmelidir. Cihazın desteklediği aktif VLAN sayısı en az 4000 olmalıdır. Port bazında VLAN tanımlanabilmelidir.
    7. Anahtar, dinamik VLAN konfigürasyonunu desteklemelidir. Yeni bir VLAN’ın tek bir anahtar üzerinde yaratılması, ağ üzerindeki diğer tüm anahtarlarda da otomatik olarak yaratılmasını sağlamalıdır.
    8. Anahtar, IEEE 802.1d “spanning tree” protokolünü desteklemelidir.
    9. Anahtar üzerinde her VLAN için farklı “spanning tree” kullanılabilmelidir. IEEE 802.1s protokolü desteklenmelidir.
    10. Anahtar, kullanıcı ve trunk portlarında spanning tree hesaplarını hızlandırabilmelidir. IEEE 802.1w protokolü desteklenmelidir.
    11. Anahtar üzerinde minimum 8 adet 10/100/1000 port ya da 8 adet 1000BaseX ya da 8 adet 10GE port, aynı kanal altında toplanıp, tek port gibi çalışabilmelidir. En az 30 adet kanal tanımlanabilmelidir. Aynı kanal içindeki portlar, farklı slotlardaki modüller üzerinden seçilebilmelidir. IEEE 802.3ad standardı desteklenmelidir.
    12. Anahtar üzerindeki bütün 10/100/1000 portlar hem half-duplex hem de full-duplex çalışabilir olmalıdır. Port hızları, 10/100/1000 şeklinde algılanabilmelidir. IEEE 802.3x standardı desteklenmelidir.
    13. Anahtar, jumboframe desteğine sahip olmalıdır. Desteklenen jumboframe’lerin uzunluğu, en az 9000 byte olmalıdır.
    14. Anahtarın 802.1Q-in-802.1Q ( VlanDoubleTagging ),Selective QinQ ve PrivateVlan desteği bulunacaktır.
    15. Anahtarın broadcast, multicast ve unicast fırtına kontrol mekanizmaları bulunucaktır.
    16. Teklif edilecek omurga anahtar, “DHCP requestbroadcast” paketlerini, ayrı bir VLAN’deki DHCP sunucuya taşıyabilmek için DHCP relay özelliğini desteklemelidir.
    17. Teklif edilecek omurga anahtar hem IPv4 hem de IPv6 için DHCP sunucu olarak kullanılabilmelidir.
    18. Anahtar DNS client ve DNS proxy olarak çalışabilmelidir.
    19. Anahtarın IEEE 802.1ab LLDP (Link Layer Discovery Protocol) veya benzeri protokol desteği bulunacaktır.
    20. Anahtar, statik IP yönlendirmeyi destekleyecektir.
    21. Anahtar hem Ipv4 hem de IPv6 çalışması için gerekli olan 6to4 ve ISATAP özelliklerine sahip olmalıdır.
    22. Anahtar, IPv4 Dinamik IP yönlendirme protokollerinden, RIP v1 ve v2, OSPF ve BGPv4 protokollerini destekleyecektir. Bu özellikler lisansa bağlı ise , teklife tüm lisanslar dahil edilecektir.Yönlendirmenin kesilmemesi için Graceful Restart GR desteği bulunmalıdır.
    23. Anahtar, IPv6 dinamik yönlendirme protokollerinden, RIPng (RFC 2080) ve OSPFv3 (RFC 2740)protokollerini destekleyecektir. Bu özellikler lisansa bağlı ise, teklife tüm lisanslar dahil edilecektir.
    24. Anahtar, hem Ipv4 hemde Ipv6 için politika tabanlı yönlendirmeyi ( policybasedrouting )destekleyecektir. Bu özellik lisansa bağlı ise, teklife tüm lisanslar dahil edilecektir.
    25. Anahtar, VRRP veya benzeri ağ geçidi yedekleme protokollerini destekleyecektir. Bu özellik lisansa bağlı ise, teklife tüm lisanslar dahil edilecektir.
    26. Anahtarın IPv4 yönlendirme tablosu, en az 512K yönlendirme bilgisini tutabilmelidir.
    27. Anahtarın IPv6 yönlendirme tablosu, en az 512K adet yönlendirme bilgisini tutabilmelidir.
    28. Anahtarın VRF-Lite (Virtual Routing and Forwarding) desteği bulunacaktır. Bu özellikler lisansa bağlı ise , teklife tüm lisanslar dahil edilecektir.
    29. Anahtar gerektiğinde ilave modül veya yazılım ile ileri düzey uygulamalar için MPLS VPN,MPLS QOS ve MPLS/VPLS Proxy desteğine sahip olabilmelidir.
    30. IGMP v1,v2,v3 ve IGMP Snooping desteklenecektir.
    31. IPv6 MLD (Multicast ListenerDiscovery) v1 ve v2 desteklenecektir. Bu özellikler lisansa bağlı ise , teklife tüm lisanslar dahil edilecektir.
    32. Anahtar üzerinde IPv6 tabanlı erişim kontrol listeleri (ACL) desteklenecektir.ACL ‘ler zaman tabanlı olabilmeli portlara,VLAN’lara ve yönlendirme tablolarına atanabilmelidir.
    33. Anahtarın IPv6 ping, telnet, traceroute özellikleri bulunacaktır.
    34. PIM-SM (PIM SparseMode) ve PIM-DM (PIM Dense Mode),DVMRP,PIM-SSM desteklenecektir.PIM-SM/DM/SSM desteği IPv6 için de desteklenecektir.
    35. Cihazın "QoS (Quality of Service)" desteği bulunmalıdır.
    36. Üçüncü seviyede (L3) DiffServCode 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.
    37. Anahtar muhtelif uygulamalar için bantgenişliği garantisi sağlamak amacıyla Strict Priority (SP),WRR (Weighted Round Robin) ve SWRR özelliklerine sahip olmalıdır.
    38. Cihaz üzerindeki her portun en az 8 adet öncelik kuyruğu bulunmalıdır.
    39. Anahtar portlarının hızları sınırlandırılabilmelidir. Tüm portlarda 64Kbps’ lık hassas hız değişim aralıkları desteklenmelidir.
    40. Anahtarın, IPv4 ve IPv6 için DHCP Snooping (Trusted DHCP server) desteği bulunacaktır. Bu sayede, anahtar üzerinden geçen kullanıcı DHCP istekleri, her bir kullanıcı için anahtar üzerinde IP ve MAC binding tablosunda tutulacaktır.
    41. Anahtarın Dynamic ARP Inspection (DAI) özelliği bulunacaktır. Bu sayede bazı tip man-in-the-middle atakları engellenebilecektir. Anahtar, üzerinden geçen tüm ARP istek ve cevaplarını incelemeli ve her ARP paketi, IP-MAC binding tablosu ile eşleştirebilmelidir. Eşleşmeyen paketler drop edilebilmelidir.
    42. Anahtarın Ping Sweep,PING-DOS,DDOS,Bluster,Zero Day, saldırılarını engelleme özelliği ve CPU koruma desteği bulunmalıdır.
    43. Anahtarın SpanningTreeRootGuard özelliği bulunacaktır. Bu sayede network yöneticisinin kontrolünde olmayan anahtarların, SpanningTree protokolü için root anahtar olması engellenebilecektir.
    44. Anahtar üzerinde bulunan her port için MAC adresi bazında kullanıcı listeleri oluşturulabilmeli ve böylece port güvenliği sağlanabilmelidir.
    45. Anahtarın IEEE 802.1x desteği bulunacak ve aşağıda belirtilen 802.1x özellikleri desteklenecektir.

• 802.1x VLAN assignment; Radius server yardımı ile port bazında kullanıcı yetkilendirme ve dinamik VLAN tahsisi

• 802.1x Guest VLAN; 802.1x uyumlu olmayan kullanıcılar ve network’e giriş için yeterli yetkiye sahip olmayan kullanıcılar GuestVLAN’a aktarılabilecektir.

• 802.1x Web yetkilendirmesi, 802.1x desteği bulunmayan kullanıcıların networke erişimlerini sağlayabilmek için http tabanlı Web browser üzerinde erişim yetkilendirmesi yapılabilecektir.

* + 1. Cihaz, paketleri L2 başlığındaki kaynak/hedef MAC adresi, L3 başlığındaki kaynak/hedef IP adresi, L4 başlığındaki TCP/UDP port numarası bilgilerine göre erişim denetiminden geçirebilmelidir.
    2. Anahtarın konsol port erişiminde farklı seviyelerde yetkiler tanımlanabilecektir. Bu sayede yetkilendirme sonrası, cihaza farklı seviyelerde (kısmi yönetim, tam yönetim, izleme gibi) erişim sağlanabilecektir.
    3. Netflow 9 ve Sflow protokol desteği bulunacaktır.
    4. Anahtarın tüm portları en az 4 adet RMON grubunu (history, statistics, alarms, events) desteklemelidir.
    5. Anahtar, SNMP v3, telnet, Secure Shell (SSH) v2 ve konsol aracılığı ile yönetilebilmeli ve gözlenebilmelidir.Bu yönetim türlerinin tamamı için Ipv6 desteği olmalıdır.
    6. Anahtarı yönetmek isteyen kişiler RADIUS ve TACACS+ sorgulama protokolü tarafından sorgulanabilmelidirler.Ipv6 için RADIUS desteği olmalıdır.
    7. TFTP yardımı ile işletim sistemi güncellemesi yapılabilmelidir.
    8. Anahtarın Syslog desteği olmalıdır.
    9. Detaylı gerçek zamanlı trafik analizi yapabilmek için port mirroring desteği bulunmalıdır. Birden fazla kaynak portu, hedef portuna ayarlanabilmelidir. Kaynak portu ile hedef portu, aynı anahtar üzerinde farklı slotlarda bulunabilmelidir.
    10. Anahtarın saat ve tarih bilgisi, ağ üzerindeki diğer tüm anahtarlarla senkron hale getirilebilecektir.
    11. Anahtar grafik tabanlı bir ağ yönetim platformu tarafından yönetilebilmelidir.
    12. Garanti süresi en az 5 yıl olacaktır.

.