

KAYSERİ BÜYÜKŞEHİR BELEDİYESİ
OMURGA ANAHTAR, KENAR ANAHTAR ve ERİŞİM NOKTASI CİHAZ ALIMI
İŞİ
TEKNİK ŞARTNAMESİ

1. Amaç ve Kapsam

Bu teknik şartname ile Kayseri Büyükşehir Belediyesi daire başkanlıklarında kullanılmak üzere omurga anahtar, kenar anahtar ve erişim noktası cihazı temin edilmesi amaçlanmaktadır.

1.1. Genel Şartlar

- 1.1.1. Temin edilecek ürünlerin tamamı yeni ve daha önce kullanılmamış olmalıdır.
- 1.1.2. Temin edilecek ürünlerde elektrikle çalışanlar 220V ile uyumlu olmalı ve bunun için gerekli bağlantı kabloları ve aparatları ürün ile birlikte verilmelidir.
- 1.1.3. Temin edilecek ürünlerin garantileri en az 2 yıl olmalıdır.
- 1.1.4. Temin edilecek ürünlerin teslimatı Bilgi İşlem Daire Başkanlığına yapılmalıdır.
- 1.1.5. Temin edilecek ürünlerin kullanımı esnasında bir arıza, hata vb. olması durumunda en fazla 2 saat içerisinde ürünlere yerinde müdahale edilmelidir.

Omurga Anahtar Tip1 (1 adet)

1. Anahtarın üzerinde none blocking çalışan en az 48 adet 1/10G SFP+ port ve 6 adet QSFP+ port bulunmalıdır.
2. Her bir SFP+ port 100Mb/1Gb/10Gb hızlarını desteklemelidir
3. Her bir QSFP+ port 4 adet 10G olarak kullanılabilmelidir. Bu şekilde çalışmıyorsa her bir QSFP+ port başına en az 4 adet SFP+ port teklif edilmelidir.
4. Anahtarlama kapasitesi en az 1.4Tb olmalıdır.
5. Anahtarın işletim performansı en az 990mpps olmalıdır.
6. Anahtar VRRP desteğine sahip olmalıdır.
7. İki anahtar yedekli çalışmayı desteklemelidir. CSF,VPC,VSS veya benzeri bir yedekleme sistemini desteklemelidir.
8. RIP, OSPF, BGP,ECMP ve PBR yönlendirme teknolojilerini desteklemelidir.
9. Layer2, Ipv4 ve Ipv6 için multicast yönlendirme olmalıdır.
10. Anahtar yetkisiz dhcp sunucuların ip dağıtımlarını önlemelidir.
11. Anahtar birden fazla porttaki veya birden fazla vlan'daki datayı bir porta yönlendirebilmelidir.
12. Anahtarın en az 9200Byte MTU desteği olmalıdır.


Serdar KAROĞLU
Bilgi Teknolojileri Şb.Sor.

13. Anahtar yedekli fan ve yedekli power desteklemeli ve tüm fan ve power slotları dolu olarak teklif edilmelidir.
14. Anahtar en az 280000 MAC adresini desteklemelidir.
15. Anahtar IPv4 için en az 20000 yönlendirmeyi desteklemelidir.
16. Anahtar IPv6 için en az 8000 yönlendirmeyi desteklemelidir.
17. Anahtar en az 4000 adet vlan desteklemelidir.
18. Anahtarın Q-in-Q desteği olmalıdır.
19. Anahtarın yönetim amaçlı konsol portu olmalıdır.
20. Anahtar 1U veya şasi tipinde teklif edilmelidir.
21. Omurga anahtar ile birlikte 40 adet LR modül, 10 adet SX modül, 20 adet SR modül ve 80 adet LH modül teklif edilmelidir. Bu modüller teklif edilen anahtarlar ile tam uyumlu olmalıdır.
22. Teklif edilen anahtar kurumda bulunan ağ yönetim yazılımı ve NAC çözümleri ile tam uyumlu olmalıdır. Mevcut Ağ yönetim yazılımına anahtarlar eklenmelidir. Bunun için gerekli lisanslar teklife dâhil edilmelidir.

Omurga Anahtar Tip2 (2 adet)

23. Anahtar üzerinde en az 24 adet PoE+ 1G port bulunmalıdır. Herhangi bir fiber uplink portu kullanıldığında bu portlardan herhangi biri kullanım dışı kalmamalıdır.
24. Anahtar modüler yapıda olmalıdır. Mevcut 24 porta ilave olarak modüler slotta 8 adet SFP+ , 2 adet QSFP ve 2 adet 25G network modülleri takılabilmelidir. 8 adet SFP+ network modül yuvası ile teklif edilmelidir.
25. Anahtarlama bant genişliği yığınlama kapasitesi hariç en az 200 Gbps olmalıdır. Anahtarın L2 anahtarlama performans değeri en az 150 Mpps olmalıdır.
26. Anahtar en az 16MB paylaşımlı bir buffer'a sahip olmalıdır.
27. Anahtarın uplink portları modüler olmalı ve en az 4 adet 1GbaseX, 8 adet 10GbaseX veya 2 adet 40GbaseX ara yüzlerini destekleyen modül opsiyonları olmalıdır. Anahtar 8 adet SFP+ seçeneği ile teklif edilmelidir.
28. Anahtar IPv4 ve IPv6 protokolleri için tıkanmasız yapıda çalışmalıdır.
29. Anahtarın modüler güç kaynağı desteği olmalıdır. İkinci bir dâhili güç kaynağı takılarak güç kaynağı yedeklemesine sahip olabilmelidir.
30. Yedek güç kaynağı anahtar çalışmaya devam ederken değiştirilebilmelidir.
31. Anahtar modüler ve N+1 yedekli çalışan fan'lara sahip olmalıdır.
32. Anahtar programlanabilir bir ASIC'e sahip olmalıdır. Yazılım güncellemesi ile ileride gereksinim desteği gerekebilecek olan yeni protokollerin de anahtarlanmasına açık olmalıdır.
33. Anahtarın kontrol ve yönetim katmanı için kullandığı işlemci mimarisi çok çekirdekli yapıda olmalıdır.
34. Anahtar 3. parti uygulamaların çalıştırılabileceği bir container altyapısı bulunmalı ve bu altyapıyı destekleyebilecek CPU ve bellek kapasitesi olmalıdır. Anahtar bu 3. Parti uygulamalar tarafından kullanılabilecek en az bir adet USB 3.0 SSD hafıza ara yüzüne sahip olmalıdır.
35. Anahtarın işletim sistemi modern programlama dillerinden NETCONF, RESTCONF ve YANG modellerini ve cihaz üzerinde Python scripting desteklemelidir.

Serdar YAROĞLU
Bilgi Teknolojileri Sb.Sor.

36. Anahtar üzerinde en az bir adet USB 2.0 ara yüz bulunmalıdır. Bu arayüz üzerinden anahtara işletim sistemi yüklemek veya log dosyalarını aktarmak mümkün olmalıdır.
37. Anahtarın 9100 byte'lık jumbo frame desteği olmalıdır.
38. Anahtarın bakır portlarında 802.3az EEE (Energy Efficient Ethernet) desteği olmalıdır.
39. Anahtar envanter yönetimi için kullanılacak bir RFID etiketine sahip olmalıdır.
40. Anahtar üzerinde veri merkezi içinde yerinin kolay bulunabilmesi için açılıp kapatılabilen mavi ışık (Blue Beacon) desteğine sahip olmalıdır.
41. Anahtar yazılımsal olarak Bluetooth desteğine sahip olmalıdır. Opsiyonel olarak bağlanacak bluetooth aparatı üzerinden anahtarın WEB ve komut ara yüzüne erişmek, log ve işletim sistemi transferi yapmak mümkün olmalıdır.
42. Her anahtar üzerinde 2 adet yığınlama portu olmalıdır. Yığınlama için kullanıcı veya uplink portları kullanılmamalı ve yığınlama çalıştırıldığında hiç bir kullanıcı portu devre dışı kalmamalıdır.
43. Stack arayüzleri ve en az 0.5m uzunluğunda stack kabloları teklife eklenmelidir.
44. Anahtar sekiz adete kadar yığılanabilmelidir.
45. Tüm yığın tek IP Adresi ve tek bir konfigürasyon üzerinden yönetilebilmeli ve yığın çalışırken yeni bir anahtarı yığına eklenebilmelidir.
46. Yığında anahtarlama bant genişliği en az 688 Gbps olmalı, yığındaki tüm anahtarlar bu bant genişliğine tam erişime sahip olmalıdır.
47. Yığındaki farklı anahtarlar üzerinden etherchannel yapmak mümkün olmalıdır.(multi-chassis etherchannel)
48. Anahtar, yığın içinde çalışırken istenildiğinde yığındaki diğer anahtarlarla güç kaynağı paylaşımı yapabilmeli, ya da istenildiğinde yığındaki güç havuzundan yararlanarak güç yedekli modda çalışabilmelidir. Güç kaynağı yığınlama olarak adlandırılan bu özellik için gerekli stack kabloları teklife dahil edilmelidir.
49. Power stack desteklenmiyorsa en az iki adet olmak üzere teklif edilen anahtarın desteklediği en yüksek power teklif edilmelidir.
50. Anahtar en az Spanning Tree (802.1d, MST, Rapid), 802.1x, 802.3af, LACP, IGMP Snooping, DHCP Snooping özellikleri için SSO (Stateful Switchover) desteklemelidir.
51. Anahtar en az 32.000 adet MAC adresi desteklenmelidir.
52. En az 4000 adet aktif VLAN desteği olmalıdır.
53. IEEE 802.1d Spanning Tree Protocol(STP), 802.1w Rapid Spanning Tree ve 802.1s Multiple Spanning Tree Protocol (MSTP) desteklenmelidir. Vlan'ler arası yük dengelemesi için 802.1d ve 802.1w protokolleri her VLAN için ayrı ayrı çalıştırılabilir.
54. Anahtar L2 loop'ları engelleme konusunda Spanning Tree yardımcı özelliklerinden, BPDU guard, Root Guard, LoopGuard özelliklerini desteklemelidir.
55. Anahtar Resilient Ethernet Protokolünü (REP) desteklemelidir.
56. Fiberoptik ara yüzlerde, bağlantıların tek yönlü olarak fiberoptik kablolama veya port hatalarından dolayı arızalanması durumunda bunu algılayan ve tek yönlü olan linkleri kapatan özelliği bulunmalıdır.
57. Anahtarın iki cihaz arasında otomatik olarak L2 trunk oluşturmak için bir protokol desteği bulunmalıdır.
58. Anahtar IEEE 802.3ad - LACP desteklemelidir. Cihaz üzerinde minimum 8 adet 10/100/1000 ya da 1000BaseX port, aynı kanal altında toplanıp, tek port gibi çalışabilmelidir.

59. Anahtar, 802.1AB protokolünü desteklemelidir. Bu sayede kendisine doğrudan bağlı diğer anahtarları öğrenme (neighbor learning) özelliğine sahip olacaktır.
60. Anahtar en az 32.000 adet IPv4 veya 16.000 adet IPv6 route bilgisini tutabilecek bir donanım yapısına sahip olmalıdır.
61. Anahtar statik yönlendirme, VLAN'ler arası IP yönlendirme ve dinamik yönlendirme protokollerinden RIP ve OSPF desteklemelidir.
62. Anahtar VRRP gibi üçüncü katman bir yedekleme protokolü desteklemelidir
63. Anahtar politika tabanlı yönlendirme (PBR) desteklemelidir.
64. Anahtar örnekleme yapmadan Netflow veya SFlow desteklemelidir. Üzerinde en az 64.000 adet flow bilgisi tutabilmelidir.
65. Anahtarın IGMP v1, v2 ve v3 desteği olmalıdır.
66. Anahtarın IGMP snooping ve MLD snooping desteği olmalıdır.
67. Anahtarın, IGMP filtering özelliği bulunacaktır. Bu sayede multicast grubuna üye olmayan kullanıcıların multicast yetkilendirmesi ve port bazında multicast yayın sınırlandırması yapılabilecektir.
68. Anahtar, RADIUS authentication, authorization ve accounting (AAA) servislerini desteklemelidir.
69. Anahtar, TACACS+ desteğiyle ağ güvenliğinin bir TACACS sunucu tarafından yönetimini desteklemelidir.
70. Cihaz, paketleri L2 başlığındaki kaynak/hedef MAC adresi, L3 başlığındaki kaynak/hedef IP adresi, L4 başlığındaki TCP/UDP port numarası bilgilerine göre erişim denetiminden (ACL) geçirebilmelidir. Cihaz üzerinde tanımlanan erişim denetim listeleri zamana bağlı olarak aktif hale getirilebilmelidir.
71. Erişim kontrol listeleri Port, VLAN ve SVI (Switched virtual interface) seviyesinde uygulanabilmelidir.
72. Erişim kontrol listeleri donanım tabanlı olarak kullanılmalıdır.
73. Anahtar en az 5000 adet ACL desteğine sahip olmalıdır.
74. Anahtar her porttan belirlenen adet kadar MAC adresinin bağlantı kurmasını sağlayabilmelidir. Belirlenen limit dışındaki MAC adresleri isteğe bağlı olarak belirlendiğinde port kapatılabilmeli veya limit dışı MAC adreslerinin bağlanması engellenebilmelidir.
75. Anahtar DHCP, ARP ve IP ataklarını engellemek için DHCP snooping, Dynamic ARP Inspection ve IP Source Guard özelliklerine sahip olmalıdır.
76. Anahtar 802.1x desteklemeli, bir RADIUS sunucu üzerinden dinamik ACL ve VLAN Ataması yapılabilmelidir. Anahtar yetkilendirme değişikliklerinde tekrar kimlik doğrulama işlemi gerektirmemelidir (CoA-Change of Authorization).
77. 802.1x desteklemeyen cihazlar için bir RADIUS sunucu üzerinden MAC adres tabanlı kimlik doğrulama yapılabilmelidir.
78. 802.1x desteklemeyen cihazlar için WEB tabanlı kimlik doğrulama işlemi yapılabilmeli ve bir HTTP sunucuya yönlendirme yapılabilmelidir.
79. Aynı porttan birden fazla istemci bağlandığında her biri için ayrı ayrı 802.1x kimlik doğrulama yapılabilmelidir.
80. Anahtarın 802.1x desteklemeyen istemciler için misafir VLAN desteği bulunmalıdır.
81. Anahtar kontrol katmanını korumak için CoPP (Control Plane Policing) desteklemelidir.
82. Anahtar hem uplink hem de downlink portlarında 802.1AE, MACSec desteklemelidir.

83. Anahtar Voice VLAN yaratılmasını destekleyecektir. Bu sayede IEEE 802.1p class of service (CoS) uyumlu IP telefonların otomatik olarak tanınması ve Voice Vlan a eklenmesine olanak sağlamalıdır.
84. Anahtar üzerindeki her portun en az 8 adet çıkış öncelik kuyruğu (Egress Queue) bulunmalı ve kuyruk uzunluklarını kontrol ederek tıkanıklıkları engelleyen otomatik sistemi bulunmalıdır.
85. Anahtarın "QoS (Quality of Service)" desteği bulunmalıdır. Üçüncü seviyede (L3) DiffServ Code Point (IP ToS/DSCP) ya da ikinci seviyede (L2) IEEE 802.1p CoS (Class of Service) ile sınıflandırılmış paketlerin öncelik değerlerini anlayabilmeli, gerektiğinde bu öncelik değerlerini değiştirebilmelidir.
86. Anahtar üzerindeki 10/100/1000 portlarının hızı sınırlandırılabilir (Rate Limiting).
87. Anahtarın IPV4 ve IPV6 için DHCP istemci ve sunucu desteği olmalıdır. Hem statik hem dinamik olarak istemcilere atamalar yapabilmelidir.
88. Anahtar uzak lokasyondaki DHCP sunuculara DHCP isteklerini iletmek için DHCP relay desteğine sahip olmalıdır. Bu özellik IPV4 ve IPV6 için desteklenmelidir.
89. Anahtarda detaylı gerçek zamanlı trafik analizi yapabilmek için VLAN ve port bazında port aynalama desteği bulunmalıdır. Anahtarın aynı anahtar üzerinde (SPAN) ve farklı anahtarlar arasında (RSPAN) aynalama yeteneği olmalıdır.
90. TFTP, FTP, SCP protokolleri ile işletim sistemi güncellemesi yapılabilir.
91. Anahtar syslog sunuculara log gönderebilmeli, hata, kaynak kullanımı ve zaman aşımı gibi bilgileri raporlayabilmelidir. Raporlanacak bilgi başlıkları seçilebilir olmalıdır.
92. Anahtarın saat ve tarih bilgisi, ağ üzerindeki diğer tüm anahtarlarla eşzaman hale getirilebilecek NTP protokolünü desteklemelidir.
93. Anahtar, SNMP v1, v2c, v3, telnet, Secure Shell (SSH) v2, HTTP (web), SSL, konsol ve ethernet yönetim portu aracılığı ile yönetilebilmeli veya gözlenebilmelidir.
94. Anahtar SNMP trap yeteneğine sahip olmalıdır.
95. En az 4 grup RMON (history, statistics, alarms, events) desteği olmalıdır. HTTP (web) yönetim sunucusu hem IPV4 hem IPV6 istemcilere servis sağlayabilmelidir.
96. Cihaz aynı anda 16 adete kadar telnet bağlantısını ve 5 SSH bağlantısını destekleyebilmelidir.
97. Anahtar 10/100/1000 bakır portlarında TDR (time domain reflector) desteklemelidir. Bu sayede cihaz, bu portlardaki kablolu hatalarını teşhis edebilmeli, kabloda kopukluk olması durumunda ne kadar uzakta olduğunu tespit edebilmelidir.
98. Anahtar L3 statik yönlendirme ve IPV4 ve IPV6 dinamik yönlendirme protokollerinden RIP, RIPng, OSPF, OSPFv3 ve IS-IS destekleyebilmelidir..
99. Anahtar en az 500 adet uygulamayı tanıyabilmeli, bu bilgileri QoS tanımlarında kullanabilmeli, anahtar üzerinde raporlayabilmeli veya netflow ve benzeri protokoller üzerinden yönetim sistemleriyle paylaşabilmelidir.
100. Anahtarın işletim sistemi yazılım seviyesini değiştirmeden belli hataları düzeltmek için üretilen yamalama (Patch) yeteneği olabilmelidir.
101. Anahtar HSRP üçüncü katman yedekleme protokolünü destekleyebilmelidir.
102. Anahtar en az 1000 adet multicast route kapasitesini destekleyebilmeli ve L3 multicast protokollerinden en az PIM-Sparse, Bidirectional PIM (PIM-BiDir), Source-Specific Multicast (SSM) ve Multicast Source Discovery Protocol (MSDP) destekleyebilmelidir.
103. Anahtar VRF-lite destekleyebilmelidir.

104. Anahtar bir uç noktaya olan erişimin kalitesini (paket kaybı, gecikme, jitter) ölçmek için IP SLA destekleyebilmelidir.
105. Teklif edilen anahtar kurumda bulunan ağ yönetim yazılımı ve NAC çözümleri ile tam uyumlu olmalıdır. Mevcut Ağ yönetim yazılımına anahtarlar eklenmelidir. Bunun için gerekli lisanslar teklife dahil edilmelidir.

Kenar Anahtar Tip1(15 Adet)

1. Cihazın üstünde en az 48 adet 1G bakır RJ45, en az 4 adet fiber SFP+ port olmalıdır.
2. Cihazın tüm bakır portları 802.3af (PoE) ve 802.3at (PoE+) standartlarını desteklemelidir. Cihaz en az 370W'a kadar PoE bütçesi sağlayabilmelidir.
3. Perpetual PoE özelliği sayesinde switch kullanıcı tarafından yeniden başlatılırken bağlı cihazlara PoE sağlamaya devam edebilmelidir.
4. Cihaz komut satırı ara yüzünü (CLI) ve Web ara yüzünü (Web UI) desteklemelidir. İstenirse bu ara yüzlere bir USB aparat aracılığıyla Bluetooth üzerinden de erişilebilmelidir.
5. En az 8 cihaza kadar yığılanabilmeli ve tek bir IP adresi üzerinden yönetilebilmelidir.
6. Cihaz aşağıdaki güvenlik özelliklerini desteklemelidir:
 - a. 802.1X, 802.1X monitör mode, Radius CoA (Change of Authorization), multi-host mode, multi-auth mode, multi-domain authentication, Guest VLAN, Failed Auth VLAN, MAC-based VLAN assignment, Wake on LAN
 - b. IPv4 ve IPv6 ACL (Güvenlik ve QoS için)
 - c. Telnet, SSH v2, Kerberos, SNMP v3
 - d. SPAN (Switch port Analyzer)
 - e. RADIUS ve TACACS+
 - f. MAB (MAC Authentication Bypass) ve Web Authentication. Bu yöntemlerde downloadable ACL de desteklenmelidir.
 - g. DHCP snooping, IP Source Guard, Dynamic ARP Inspection
 - h. Port security
 - i. IGMP filtering
 - j. sFlow
 - k. IPv6 First Hop Security (RA Guard, DHCPv6 Guard, Source/Prefix Guard, Destination Guard, ND Multicast Suppress)
7. Cihaz RSTP, PVRST+ ve MSTP desteklemelidir.
8. Cihaz aşağıdaki QoS özelliklerini desteklemelidir:
 - a. Port başına çıkış yönünde 8 kuyruk
 - b. Ingress policing
 - c. DSCP mapping ve filtering
 - d. Traffic classification
 - e. AutoQoS
 - f. SRR ve WTD
 - g. 802.1p CoS marking ve reclassification
9. Cihaz 802.3az Energy Efficient Ethernet standardını desteklemelidir.
10. Cihaz aşağıdaki operasyonel kolaylık özelliklerini veya benzerini desteklemelidir:

Serdar YAROĞLU
Bilgi Teknolojileri Şb.Sor.

- a. LACP
 - b. UDLD
 - c. BPDU Guard, STP Root Guard
 - d. Storm control (broadcast, multicast ve unicast için)
 - e. Local Proxy ARP ve Private VLAN Edge
 - f. IGMP snooping ve MLD v1 ve v2 snooping
 - g. Voice VLAN
 - h. Layer 2 traceroute
 - i. TFTP
 - j. NTP
 - k. Dying Gasp
11. Cihaz Jumbo frame desteklemelidir.
12. Cihaz minimum aşağıdaki spesifikasyonlara sahip olmalıdır
- a. 176 Gbps "Switching bandwidth", 130 Mpps "Forwarding rate" (64 byte paketler için). ("line-rate forwarding" desteklemelidir).
 - b. 16000 Mac adresi
 - c. IPv4: 542 host girdisi, 256 unicast rota
 - d. IPv6: 414 host girdisi, 128 unicast rota
 - e. 1024 IGMP ve MLD grubu
 - f. 600 Ipv4/Ipv6/MAC ACL girdisi
 - g. 4096 VLAN ID, 256 aktif VLAN
 - h. 64 SVI
 - i. 64 STP instance
 - j. 4 SPAN oturumu
 - k. 1,5 MB buffer
13. Cihazın MTBF değeri en az 850000 saat olmalıdır.
14. Cihaz en az -5° - +45°C sıcaklık ve %5 - %90 (40°C'de) bağıl nem oranı aralığında çalışabilmelidir.
15. Teklif edilen anahtar kurumda bulunan ağ yönetim yazılımı ve NAC çözümleri ile tam uyumlu olmalıdır. Mevcut Ağ yönetim yazılımına anahtarlar eklenmelidir. Bunun için gerekli lisanslar teklife dahil edilmelidir.

Kenar Anahtar Tip2(15 Adet)

1. Cihazın üstünde en az 24 adet 1G bakır RJ45, en az 4 adet fiber SFP+ port olmalıdır.
2. Cihazın tüm bakır portları 802.3af (PoE) ve 802.3at (PoE+) standartlarını desteklemelidir. Cihaz en az 195W'a kadar PoE bütçesi sağlayabilmelidir.
3. Perpetual PoE özelliği sayesinde switch kullanıcı tarafından yeniden başlatılırken bağlı cihazlara PoE sağlamaya devam edebilmelidir.
4. Teklif edilen anahtar fan sız olmalıdır.
5. Cihaz komut satırı ara yüzünü (CLI) ve Web ara yüzünü (Web UI) desteklemelidir. İstenirse bu ara yüzlere ek bir USB aparat aracılığıyla Bluetooth üzerinden de erişilebilmelidir.
6. En az 8 cihaza kadar yığılanabilmeli ve tek bir IP adresi üzerinden yönetilebilmelidir.

Serdar YAROĞLU
Bilgi Teknolojileri Şb.Sor.

7. Cihaz aşağıdaki güvenlik özelliklerini desteklemelidir:
 - a. 802.1X, 802.1X monitor mode, Radius CoA (Change of Authorization), multi-host mode, multi-auth mode, multi-domain authentication, Guest VLAN, Failed Auth VLAN, MAC-based VLAN assignment, Wake on LAN
 - b. IPv4 ve IPv6 ACL (Güvenlik ve QoS için)
 - c. Telnet, SSH v2, Kerberos, SNMP v3
 - d. SPAN (Switch port Analyzer)
 - e. RADIUS ve TACACS+
 - f. MAB (MAC Authentication Bypass) ve Web Authentication. Bu yöntemlerde downloadable ACL de desteklenmelidir.
 - g. DHCP snooping, IP Source Guard, Dynamic ARP Inspection
 - h. Port security
 - i. IGMP filtering
 - j. sFlow
 - k. IPv6 First Hop Security (RA Guard, DHCPv6 Guard, Source/Prefix Guard, Destination Guard, ND Multicast Suppress)
8. Cihaz RSTP, PVRST+ ve MSTP desteklemelidir.
9. Cihaz aşağıdaki QoS özelliklerini desteklemelidir:
 - a. Port başına çıkış yönünde 8 kuyruk
 - b. Ingress policing
 - c. DSCP mapping ve filtering
 - d. Traffic classification
 - e. AutoQoS
 - f. SRR ve WTD
 - g. 802.1p CoS marking ve reclassification
10. Cihaz 802.3az Energy Efficient Ethernet standardını desteklemelidir.
11. Cihaz aşağıdaki operasyonel kolaylık özelliklerini veya benzerini desteklemelidir:
 - a. LACP
 - b. UDLD
 - c. BPDU Guard, STP Root Guard
 - d. Storm control (broadcast, multicast ve unicast için)
 - e. Local Proxy ARP ve Private VLAN Edge
 - f. IGMP snooping ve MLD v1 ve v2 snooping
 - g. Voice VLAN
 - h. Layer 2 traceroute
 - i. TFTP
 - j. NTP
 - k. Dying Gasp
12. Cihaz Jumbo frame desteklemelidir.
13. Cihaz minimum aşağıdaki spesifikasyonlara sahip olmalıdır
 - a. 128 Gbps "Switching bandwidth", 95 Mpps "Forwarding rate" (64 byte paketler için). ("line-rate forwarding" desteklemelidir).
 - b. 16000 Mac adresi
 - c. IPv4: 542 host girdisi, 256 unicast rota
 - d. IPv6: 414 host girdisi, 128 unicast rota
 - e. 1024 IGMP ve MLD grubu
 - f. 600 Ipv4/Ipv6/MAC ACL girdisi

- g. 4096 VLAN ID, 256 aktif VLAN
 - h. 64 SVI
 - i. 64 STP instance
 - j. 4 SPAN oturumu
 - k. 1,5 MB buffer
14. Cihazın MTBF değeri en az 690000 saat olmalıdır.
 15. Cihaz en az -5° - +45°C sıcaklık ve %5 - %90 (40°C'de) bağıl nem oranı aralığında çalışabilmelidir.
 16. Teklif edilen anahtar kurumda bulunan ağ yönetim yazılımı ve NAC çözümleri ile tam uyumlu olmalıdır. Mevcut Ağ yönetim yazılımına anahtarlar eklenmelidir. Bunun için gerekli lisanslar teklife dahil edilmelidir.

Kenar Anahtar Tip3 (20 Adet)

1. Cihazın üstünde en az 10 adet 1G bakır RJ45, en az 2 adet fiber SFP port olmalıdır.
2. Cihazın sekiz bakır portu 802.3af (PoE) ve 802.3at (PoE+) standartlarını desteklemelidir. Cihaz en az 120W'a kadar PoE butcesi sağlayabilmelidir.
3. Perpetual PoE özelliği sayesinde switch kullanıcı tarafından yeniden başlatılırken bağlı cihazlara PoE sağlamaya devam edebilmelidir.
4. Cihaz komut satırı ara yüzünü (CLI) ve Web ara yüzünü (Web UI) desteklemelidir. İstenirse bu ara yüzlere ek bir USB aparat aracılığıyla Bluetooth üzerinden de erişilebilmelidir.
5. En az 8 cihaza kadar yığılanabilmeli ve tek bir IP adresi üzerinden yönetilebilmelidir.
6. Cihaz aşağıdaki güvenlik özelliklerini desteklemelidir:
 - a. 802.1X, 802.1X monitör mode, Radius CoA (Change of Authorization), multi-host mode, multi-auth mode, multi-domain authentication, Guest VLAN, Failed Auth VLAN, MAC-based VLAN assignment, Wake on LAN
 - b. IPv4 ve IPv6 ACL (Güvenlik ve QoS için)
 - c. Telnet, SSH v2, Kerberos, SNMP v3
 - d. SPAN (Switch port Analyzer)
 - e. RADIUS ve TACACS+
 - f. MAB (MAC Authentication Bypass) ve Web Authentication. Bu yöntemlerde downloadable ACL de desteklenmelidir.
 - g. DHCP snooping, IP Source Guard, Dynamic ARP Inspection
 - h. Port security
 - i. IGMP filtering
 - j. sFlow
 - k. IPv6 First Hop Security (RA Guard, DHCPv6 Guard, Source/Prefix Guard, Destination Guard, ND Multicast Suppress)
7. Cihaz RSTP, PVRST+ ve MSTP desteklemelidir.
8. Cihaz aşağıdaki QoS özelliklerini desteklemelidir:
 - a. Port başına çıkış yönünde 8 kuyruk
 - b. Ingress policing


Serdar YAROĞLU
Bilgi Teknolojileri Şb.Sor.

- c. DSCP mapping ve filtering
 - d. Traffic classification
 - e. AutoQoS
 - f. SRR ve WTD
 - g. 802.1p CoS marking ve reclassification
9. Cihaz 802.3az Energy Efficient Ethernet standardını desteklemelidir.
10. Cihaz aşağıdaki operasyonel kolaylık özelliklerini veya benzerini desteklemelidir:
- a. LACP
 - b. UDLD
 - c. BPDU Guard, STP Root Guard
 - d. Storm control (broadcast, multicast ve unicast için)
 - e. Local Proxy ARP ve Private VLAN Edge
 - f. IGMP snooping ve MLD v1 ve v2 snooping
 - g. Voice VLAN
 - h. Layer 2 traceroute
 - i. TFTP
 - j. NTP
 - k. Dying Gasp
11. Cihaz Jumbo frame desteklemelidir.
12. Cihaz fan sız olmalıdır.
13. Cihaz minimum aşağıdaki spesifikasyonlara sahip olmalıdır
- a. 20 Gbps "Switching bandwidth", 14 Mpps "Forwarding rate" (64 byte paketler için). ("line-rate forwarding" desteklemelidir).
 - b. 16000 Mac adresi
 - c. IPv4: 542 host girdisi, 256 unicast rota
 - d. IPv6: 414 host girdisi, 128 unicast rota
 - e. 1024 IGMP ve MLD grubu
 - f. 600 Ipv4/Ipv6/MAC ACL girdisi
 - g. 4096 VLAN ID, 256 aktif VLAN
 - h. 64 SVI
 - i. 64 STP instance
 - j. 4 SPAN oturumu
 - k. 1,5 MB buffer
14. Cihazın MTBF değeri en az 1700000 saat olmalıdır.
15. Cihaz en az -5° - +45°C sıcaklık ve %5 - %90 (40°C'de) bağıl nem oranı aralığında çalışabilmelidir.
16. Teklif edilen anahtar kurumda bulunan ağ yönetim yazılımı ve NAC çözümleri ile tam uyumlu olmalıdır. Mevcut Ağ yönetim yazılımına anahtarlar eklenmelidir. Bunun için gerekli lisanslar teklife dahil edilmelidir.

Kablosuz Erişim Cihazı (20 Adet)

1. Önerilecek olan kablosuz ağ cihazı (kablosuz erişim noktası), 2,4 ve 5 GHz frekans bandında çalışabilecektir.
2. Kablosuz erişim noktası, teklif edilen merkez kablosuz ağ kontrol cihazı tarafından yönetilebilmelidir.

Serdar YARÖĞLU
Bilgi Teknolojileri Şb.Sor.

3. Kablosuz erişim noktası, yüklenecek yazılım ile en az 25 kablosuz erişim noktasını kontrol edebilmelidir.
4. Kablosuz erişim noktasını, en az 400 cihaz bağlanabilmelidir.
5. Kablosuz erişim noktası üzerindeki kullanıcı trafiği, merkez kablosuz ağ kontrol cihazı üzerinden, ağa iletilmelidir.
6. Cihaz, kablosuz kontrol cihazı tarafından yönetilip istenilen ssid lerin trafiğini merkezi, istenilen ssid lerin trafiği lokal olarak anahtarlayabilmelidir.
7. Kablosuz erişim noktası, 2.4Ghz bandında ETSI standartlarında 13 adet çalışma kanalını desteklemelidir. 3 adet kablosuz erişim noktası aynı ortamda yan yana frekans örtüşmesi olmadan çalışabilmelidir.
8. Kablosuz erişim noktası, bir ve ikinci nesil IEEE 802.11ac, IEEE 802.11n, IEEE 802.11a IEEE 802.11b ve IEEE 802.11g standartlarını tam uyumlu olarak destekleyecektir.
9. Cihaz üzerindeki kullanıcılar maksimum 867 Mbps hıza ulaşabilmelidir.
10. Kablosuz erişim noktası, IEEE 802.11n için, en az 3x3 multiple-input, multiple-output (MIMO), 2 spatial streams, 802.11 dynamic frequency selection (DFS), maximal ratio combining (MRC), cyclic shift diversity (CSD) ve 20, 40 ve 80 MHz kanallarını desteklemelidir.
11. Cihaz kullanıcıları kesintisiz ve sorunsuz video yayın alabilmesi için multicast video yayını unicast olarak kullanıcılara gönderebilmelidir ve bu trafiği kablosuz erişim noktası üzerinde unicast'e çevirmelidir.
12. Kablosuz erişim noktası, hızlı roaming özelliklerine sahip olmalıdır.
13. Kablosuz erişim noktası üzerinde, 1 adet 10/100/1000BASE-T portu (RJ-45) bulunmalıdır.
14. Kablosuz erişim noktası, 48 V DC güç kaynağı ile çalıştırılabilir, ya da IEEE 802.3af veya benzeri bir yöntemle, UTP kablo üzerinden de beslenebilmelidir.
15. Cihazın çıkış gücü (transmit power), ETSI standartlarına uygun olmalıdır. Gerektiğinde çıkış gücü, daha düşük bir seviyeye ayarlanabilmelidir.
16. Kablosuz erişim noktası üzerinde, 2.4 Ghz için entegre 3.0 dBi kazançlı, 5 Ghz için entegre 5.0 dBi kazançlı, omni-directional (yaklaşık 360°) dahili anten bulunmalıdır.
17. Kablosuz erişim noktası üzerinde, IEEE 802.1Q VLAN tagging (VLAN trunking) desteği bulunmalıdır.
18. Kablosuz erişim noktası üzerinde, en az 16 adet VLAN (Virtual LAN) tanımlanabilmelidir.
19. Kablosuz erişim noktası üzerinde, en az 16 adet SSID (service set identifier) tanımlanabilmeli ve her VLAN için farklı SSID tahsis edilebilmelidir.
20. Kablosuz erişim noktası, IEEE 802.1p önceliklendirme standardını desteklemelidir.
21. Kablosuz erişim noktası üzerinde, işletim sistemi ve konfigürasyon dosyalarını tutmak vb. Amacıyla, 1GB RAM ve 256 MB flash bellek bulunmalıdır.
22. Kablosuz erişim noktası, 40 ve 128 bit uzunluğundaki IEEE 802.11 WEP şifrelerini (key) desteklemelidir.
23. Kablosuz erişim noktası, Wi-Fi Protected Access (WPA) ve WPA2 sertifikasyon yöntemlerini desteklemelidir. WPA için TKIP (temporal key integrity protocol) ve WPA2 için AES (advanced encryption standart) şifreleme desteği bulunmalıdır.
24. Kablosuz erişim noktası, IEEE 802.1x authentication desteğine sahip olmalıdır.
25. Kablosuz erişim noktası, IEEE 802.11i güvenlik standardını desteklemelidir.

26. Kablosuz erişim noktası üzerinde, cihazın durumunu, ethernet bağlantısının durumunu ve aktivitesini, kablosuz bağlantının durumunu ve aktivitesini ayrı ayrı gösteren LED ler bulunmalıdır.
27. Kablosuz erişim noktası üzerindeki konfigürasyon, gerektiğinde tek bir butona basarak silinebilmeli ve fabrika çıkış değerlerine dönülebilmelidir.
28. Cihazın duvara, tavana ya da masa üstüne monte edilmesini sağlayan kitler birlikte verilecektir. Cihaz, kilitlenebilmeli ve monte edildiği yerden hırsızlık vb. nedenlerle sökülmesi engellenebilmelidir.
29. Cihazın çevre sıcaklığı, 0 °C / +40 °C arasında olmalıdır. %10 / %90 nem aralığında çalışabilmelidir.
30. Teklif edilen kablosuz erişim cihazı kurumda bulunan kablosuz kontroller cihazı ile tam uyumlu olmalıdır. Ürünler mevcut kontroller cihazına entegre edilerek çalıştırılmalıdır. Bunun için lisans gerekiyorsa teklife dâhil edilmelidir.
31. Teklif edilen kablosuz erişim cihazı ve teklif edilen anahtarlar aynı üreticinin ürünü olmalıdır.


Serdar YAROĞLU
Bilgi Teknolojileri Şb.Sor.