|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Satınalan Birim** | Bilgi İşlem Daire Başkanlığı | | |
| **Talep Eden Birim** | BİLGİ İŞLEM DAİRE BAŞKANLIĞI | | |
| **Talep Eden Birim**  **Sorumlusu** |  | |  |
| **Dosya Numarası** | 2017-13 | | |
| **Satınalma Usulü** | Yaklaşık maliyet esas olmak üzere piyasa fiyat araştırması | | |
| **Satınalma Memuru** | Zafer CAN | **Tel** : 0224 294 28 23 | |
| **Fax**: 0224 294 05 01 | |
| **E-mail**:zafercan@uludag.edu.tr | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Sıra No** | **Mal/Hizmet Cinsi** | **Mal/Hizmet Özellikleri** | **Miktarı** |
| **Donanım** | | | |
| **1-** | Omurga Anahtar Cihazı | 1\* 48 adet SFP+ port ve 6 adet 40 GB QSFP port | 1Adet |
| **2-** | Omurga Anahtar Cihazı | 1\* 48 adet  10/100/100BaseT ethernet port | 1 Adet |
| **3-** | Modül | 1 GB LX SFP | 10 Adet |

**Üniversitemiz Güvenlik Merkezi bünyesinde bulunan** Kamera sistemlerinin kullanılmak üzere Omurga Anahtar Cihazı ve Modül alımı için teklifler **24/11/2017** tarih ve saat **17:00** ye kadar U.Ü. Rektörlüğü Bilgi İşlem Daire Başkanlığına elden teslim edileceği gibi posta yoluyla da gönderilebilir. (**Not:** **Fax ile gönderilen teklifler geçerli sayılmayacaktır**.)

1. Teklif mektubu imzalı ve kaşeli olmalıdır.
2. Teklifin hangi tarihe kadar geçerli olduğu belirtilmelidir.
3. Sipariş sonrasında mal/hizmetin kaç günde teslim edileceği belirtilmelidir.
4. Teklif mektubuna dosya numarası yazılmalıdır.
5. Kısmi teklif verilmeyecektir.
6. Mal/Hizmetle ilgili her türlü giderler (Montaj, Demontaj, Araç, nakliye, sigorta, vergi, vb.) tedarikçiye aittir.
7. Teklifler **KDV hariç** olarak **TL** cinsinden verilmelidir. (TL cinsinden verilmeyen teklifler değerlendirmeye alınmayacaktır.)
8. Mal/Hizmet ile ilgili Garanti verilmelidir. (4077 sayılı Tüketici Korunması hakkında kanun ve ilgili mevzuat gereği)
9. Teklifler sıra numaralarına göre verilecektir.
10. Sipariş edilen mal/hizmetin teklifte belirtilen tarihe kadar teslim edilmesi , belirtilen tarihten sonra teslim edilmek istenilmesi halinde idare tarafından mal/hizmetin kabulü yapılmayacaktır.
11. **Aşağıda idare tarafından standart hale getirilen teklif mektubu eksiksiz doldurulup gönderilmesi halinde geçerli sayılacaktır.**

**Adres: Uludağ Üniversitesi Rektörlüğü – Bilgi İşlem Daire Başkanlığı Görükle Kampusü 16059 Nilüfer / BURSA**

**Tel : (0224) 294 05 00**

**Fax : (0224) 294 05 01**

**TEKLİF MEKTUBU**

**ULUDAĞ ÜNİVERSİTESİ REKTÖRLÜĞÜ**

**BİLGİ İŞLEM DAİRE BAŞKANLIĞINA**

**Tarih: …./…./2017**

|  |  |
| --- | --- |
| **Teklif Vermeye Yetkili Kişinin;** | |
| **Adı ve Soyadı** |  |
| **Firma Adı** |  |
| **Açık Tebligat Adresi** |  |
| **Vergi Dairesi ve Vergi Numarası** |  |
| **Telefon ve Fax Numarası** |  |
| **Elektronik Posta Adresi** |  |

|  |  |
| --- | --- |
| **Teklife İlişkin Kurum Dosya Numarası:** | |
| **Sıra No** | **Mal/Hizmet Cinsi** | **Miktarı** | **Birim Fiyatı** | **Toplam** |
| **1-** |  |  |  |  |
| **2-** |  |  |  |  |
| **3-** |  |  |  |  |
| **4-** |  |  |  |  |
| **5-** |  |  |  |  |
| **6-** |  |  |  |  |

**1-** Yukarıda belirtilen **( …… Kalem )** mal/hizmet alımına ait teklifimizi **KDV** **hariç** ……………….. **TL** bedel karşılığında vermeyi kabul ve taahhüt ediyorum/ediyoruz.

**2-**Teklifimiz **…./…./2017**  tarihine kadar geçerlidir.

**3-**Söz konusu mal/hizmet idarece tarafımıza sipariş verilmesinden sonra **……………. takvim günü içerisinde** teslim edilecektir.

**4-** 4077 Sayılı Tüketici Koruması hakkında kanun ve ilgili mevzuat hükümlerini kabul ediyor, mal/hizmet için ……. (gün/ay/yıl) garanti taahhüt ediyorum.

**5-** Teklifimizin kabul edilmesi halinde sipariş yazısının, yukarıda yer alan; 🟋

**🞎** Elektronik posta adresime veya faks numarama tebligat yapılmasını kabul ediyorum.

**🞎** Elektronik posta adresime veya faks numarama tebligat yapılmasını kabul etmiyorum.

🟋**Teklif veren istekli kabul ettiği seçeneği yazacaktır.**

**Teklif Vermeye Yetkili Kişinin;**

**Adı ve Soyadı:**

**İmzası:**

**Firma Kaşe**

**TEKNİK ŞARTNAME**

1. **GİRİŞ:** Bu şartname, Uludağ Üniversitesi Güvenlik Merkezi kamera sistemlerinde kullanılmak üzere alımı yapılacak cihazların teknik özelliklerini içerir.

1\* 48 adet SFP+ port ve 6 adet 40 GB QSFP port

1\* 48 adet  10/100/100BaseT ethernet port

10 adet 1 GB LX SFP modül

# Teknik Özellikler:

# OS6900-X72

1.    Teklif edilecek anahtar, maksimum konfigürasyon ile 48 adet SFP+ tabanlı port ve 6 adet 40 Gb QSFP port desteklemelidir. Bu yuvalara, 40GBASE-LR, 40GBASE-SR, 10GBASE-LR, 10GBASE-SR,1000BASE-LX/LH, 1000BASE-SX fiber arayüzleri takılıp çıkartılabilir olmalıdır.

2.    Anahtar, N+1 güç kaynağı yedeklemesine sahip olmalı ve yedekli olarak teklif edilmelidir. Bu güç kaynakları cihaz çalışırken söküp takılabilmelidir.

3.    Anahtar kablo hızında ve kesintisiz olmalıdır ve switch fabric değeri en az 1440 Gbps olmalıdır. Anahtarın paket iletim hızı en az 1.4 Gpps olmalıdır.

4.    Cihazın gecikme değeri 650 ns altında olmalıdır.

5.    Anahtar üzerinde desteklenen mac adres sayısı en az 128 bin adet olmalıdır.

6.    Anahtar üzerinde IEEE 802.1Q (Virtual LAN) standartı desteklenmelidir ve desteklenen aktif vlan  sayısı en az 4000 adet olmalıdır. Ayrıca anahtar üzerinde port bazında vlan politikaları uygulanabilmelidir. Anahtar Private Vlan/Port Mapping özelliğini desteklemelidir.

7.    Anahtar ağ üzerindeki kaynakların kullanımının ayarlanabilmesi için IEEE 802.1p protokolünü desteklemelidir. Anahtar servis türlerinin bilgilerini ayrıştırabilmeli ve aynı zamanda bu bilgileri işaretleyebilmelidir. Anahtar işaretlenen bu bilgileri WRED (Weighted RoundEarly Dedection) ya da benzeri bir protokol yardımı ile ilgili kuyruklara (queue) anahtarlayabilmelidir.

8.    Ağ topolojisi üzerinde gereksinimlere göre bant genişliğini arttırmak amacıyla anahtar IEEE 802.3ad link aggregation protokolünü desteklemelidir. Böylece portlar belirli bir grup içerisinde toplanarak yüksek bant genişliği elde edilecektir.  Anahtar en az 256 adet link aggregation grubunu desteklemelidir ve her bir grubun içerisinde en az 16 adet port toplanabilmelidir. Oluşturulan grup içerisindeki portlardan herhangi birinin arızalanması durumunda grup bütünlüğü bozulmamalıdır.

9.    Anahtar üzerinde dinamik VLAN uygulamaları desteklenmelidir. Gerektiği durumlarda tanımlanan yeni bir VLAN’ın omurga anahtara bağlı diğer anahtarlar üzerinde MVRP (Multiple Vlan Registration Protocol) veya benzeri bir protokol yardımı ile otomatik olarak oluşturulması sağlanabilmelidir.

10. Anahtar üzerinde IEEE 802.1Q-in-802.1Q protokolü desteklenmelidir.

11. Anahtar üzerinde IEEE 802.1d STP (Spanning-Tree Protocol) ve IEEE 802.1s MSTP (Multiple Spanning-Tree Protocol) protokolünü desteklemelidir. Anahtar kullanıcı ve trunk  portlarında STP hesaplamalarını hızlandırabilmek amacıyla IEEE 802.1w RSTP (Rapid Spanning-Tree Protocol) protokolünü desteklemelidir. Anahtar üzerinde istenmeyen STP paketlerinin durdurulması amacıyla BPDU (Bridge Protocol Data Unit) paketlerinin istenilen arayüzden alınması, gönderilmesi ve filtrelenebilmesi desteklenmelidir. STP kök anahtarını koruyacak mekanizmalar anahtar üzerinde var olmaldır.

12. Anahtar jumbo frame özelliğini desteklemelidir. Desteklenen jumbo frame’lerin uzunluğu en az 9000 byte olmalıdır.

13. Anahtar kullanıcı portlarında broadcast fırtınalarını önleyerek ağ üzerindeki kullanılabilir bant genişliğini en uygun şekilde kullanabilmelidir. Anahtar üzerinde unicast ve multicast baskınlarına karşı koruma mekanizması olacaktır.

14. Anahtar üzerinde IEEE 802.1ab LLDP (Layer Link Discovery Protocol) desteği bulunacaktır.

15. Anahtar ağ üzerinde yedekli bir yapıyı destekleyebilmek amacıyla VRRP (Virtual Router Redundancy Protocol) ya da benzeri bir yedeklilik protokolünü destekleyebilmelidir.

16. Anahtar statik yönlendirme yapabilmelidir. Ripv1 , Ripv2 protokollerini desteklemelidir. Anahtar dinamik yönlendirme protokollerinden OSPF ve BGPv4 protokollerini  destekleyecektir. Anahtar üzerinde hardware bazında 12000 adet rota bilgisi tutulabilmelidir. Ayrıca anahtar üzerinde politika bazlı yönlendirmeler de yapılabilmelidir.

17. Anahtar MPLS şebekelerde rota bilgilerinin karışmaması için üzerinde Sanal Yönlendirme Aktarma (Virtual Routing Forwarding VRF) desteği bulunmalıdır.

18. Anahtar ağ üzerinde erişim kısıtlamaları yapabilmek amacıyla erişim denetim listelerini (Access Control List) desteklemelidir. Bu amaçla anahtar kullanıcıların belirli kaynaklara erişimini engelleyebilmelidir. Anahtar üzerinde yapılan erişim kısıtlamaları L2/L3/L4 seviyesinde olabilmelidir.

19. Anahtar donanımsal olarak ipv6 anahtarlama ve yönlendirme yeteneğine sahip olmalıdır. Anahtar ipv6 tabanlı dinamik yönlendirme protokollerinden OSPFv3 protokolünü destekleyecektir.

20. Anahtar üzerinde ipv6 tabanlı politika bazlı yönlendirmeler desteklenmelidir.

21. Anahtar üzerinde ipv6 tabanlı erişim denetim listeleri (Access Control List)  ve servis önceilklendirme (Quality Of Services) protokolleri desteklenmelidir.

22. Anahtar ağ üzerindeki gereksiz trafiğin engellenmesi amacıyla multicast anahtarlama ve multicast yönlendirme yapabilmelidir. Bu amaçla anahtar IGMPv1/v2/v3 ve IGMP Snooping v1/v2/v3 standartlarını destekleyecektir. Anahtar ayrıca dinamik multicast yönlendirme RFC 2362 PIM-Sparse Mode, RFC 3973 PIM-Dense Mode ve RFC 3569 PIM-SSM (Source Specific Multicast) protokollerini destekleyebilmelidir.

23. Anahtar üzerinde ileri seviye uygulamalar için GRE (Generic Routing Encapsulation) özellikleri desteklenmelidir.

24. Anahtar kullanıcı portları üzerinde istenmeyen bir DHCP (Dynamic Host Configuration Protocol) sunucusunun bağlanmasını önlemek amacıyla DHCP snooping özelliğini desteklemelidir.

25. Anahtar üzerinde dinamik DOS (Denial Of Service) ataklarına karşı koruması olacaktır. Anahtar üzerinde desteklenen koruma teknikleri ve protokolleri detaylı bir şekilde ayrıntılı olarak açıklanacaktır.

26. Anahtar üzerinde IGMP (Internet Group Management Protocol) protokolü filtreleme özelliği bulunmalıdır. Bu sayede anahtar üzerinde multicast domain gruplarına üye olmayan kullanıcıların multicast yetkilendirmesi ve sınırlandırılması yapılabilecektir.

27. Anahtar ağ üzerinde kendisine bağlı olan diğer anahtarların öğrenme amacıyla neighbor discovery özelliğine sahip olmalıdır.

28. Anahtar üzerinde tüm portlar en az 4 adet RMON (Remote Monitoring) grubunu desteklemelidir.

29. Anahtar telnet, console portu ve  web arayüzü ile yönetilebilmelidir. Ayrıca anahtar üzerinde SNMPv1/v2/v3 (Simple Network Management Protocol) protokolü desteklenmelidir.

30. Anahtar üzerinde konsol port erişiminde farklı seviyelerde yetkilendirmeler tanımlanabilmelidir. Böylece anahtar üzerinde konfigürasyon yönetimi ve erişim kısmi yada tam yönetim şeklinde yapılabilecektir.

31. Anahtar ağ üzerindeki güvenliği sağlamak amacıyla, ağa bağlanan kullanıcılarının yetkilendirilmesi ve erişim politikalarının uygulanabilmesi için IEEE 802.1x protokolünü desteklemelidir. IEEE 802.1x protokolü ile bir yetkilendirme yazılımından ya da radius sunucusundan belirlenen izinler ile kullanıcı bazlı yetkilendirme yapılabilmelidir. Anahtar dinamik olarak VLAN yönlendirmelerini destekleyebilecektir.

32. Anahtarı yönetmek ve konfigüre etmek isteyen kullanıcılar Radius ve TACACS+ protokolleri tarafından sorgulanabilmelidir.

33. Anahtar üzerinde gerektiğinde TFTP (Trivial File Transfer Protocol) protokolü ile yazılım dosyası güncellemesi, konfigürasyon dosyası saklanabilmesi yapılabilmelidir. Ayrıca anahtar FTP (File Transfer Protocol) client özelliğini destekleyecektir.

34. Anahtar ağ üzerindeki trafiği analiz edebilmek amacıyla port aynalama (mirroring) özelliğini desteklemelidir. Anahtar üzerinde belirlenen bir hedef portuna birden fazla kaynak portu aynalanabilmelidir (mirroring).

35. Anahtarın üzerindeki saat ve tarih bilgileri ağ üzerindeki diğer anahtarların saat ve tarih bilgileri ile senkron olabilmelidir. Bu amaçla anahtar NTP (Network Time Protocol) veya benzeri bir protokolü desteklemelidir.

36. Anahtarın, SDN (Software Defined Network) ağlarda kullanılan Open Flow desteği bulunacaktır.

37. Anahtar 19 inç Kabine montajı için gerekli parçaları ile sağlanacaktır.

**6860-48 Anahtar Özellikleri:**

38. Anahtar üzerinde en az 48 adet 10/100/1000BaseT ethernet portu ve en az 4 adet SFP, SFP+ veya XFP tabanlı yuva bulunmalıdır. Bu yuvalara 10GBASE-LR, 10GBASE-SR, 1000BASE-LX/LH, 1000BASE-SX fiber arayüzleri takılıp çıkartılabilir olmalıdır.

39. Anahtar, gerektiğinde bir güç kaynağı takılarak, güç kaynağı yedeklemesine sahip olabilmelidir.

40. Anahtar 8 adet cihaza kadar sanal şase yapılabilmelidir. Sanal Şase için talep edilen kullanıcı ve uplink portları kullanılmamalıdır. Anahtar üzerinde en az 2 adet yığınlama arayüzü bulunmalıdır. Yığındaki anahtarlar arasındaki band genişliği en az 80 Gbps olmalıdır. Anahtar ile gerekli yığınlama kablosu beraber teklif edilmelidir. Yığın içindeki anahtarlardan birisinin arızalanması durumunda, yığın içindeki diğer anahtarlar, çalışmaya devam edebilmelidir.

41. Yığın grubu içindeki anahtarların işletim sistemi, her bir anahtarın işletim sisteminin ayrı ayrı yükseltilmesine gerek olmadan, bir defada yükseltilebilmeli ve yığın grubu tek IP ile yönetilebilmelidir.

42. Anahtar kablo hızında ve kesintisiz olmalıdır ve anahtarlama bant genişliği en az 256 Gbps olmalıdır. Anahtarın L2 anahtarlama performans değeri en az 190 Mpps olmalıdır.

43. Anahtar üzerinde desteklenen mac adres sayısı en az 48 bin adet olmalıdır.

44. Anahtar üzerinde IEEE 802.3 (10BaseT Ethernet), 802.3z (1000BaseX), 802.3ab (1000BaseT) standartları desteklemelidir. Ayrıca anahtar üzerinde IEEE 802.3ae 10 Gigabit Ethernet standartı desteklenecektir. 10 Gigabit Ethernet standartları için 10GB-LR, 10GB-SR, 10GB-ER arayüzleri desteklenecektir.

45. Anahtar üzerinde IEEE 802.1Q (Virtual LAN) standartı desteklenmelidir ve desteklenen aktif vlan  sayısı en az 4000 adet olmalıdır. Ayrıca anahtar üzerinde port bazında vlan politikaları uygulanabilmelidir. Anahtar Private Vlan/Port Mapping özelliğini desteklemelidir.

46. Anahtar ağ üzerindeki kaynakların kullanımının ayarlanabilmesi için IEEE 802.1p protokolünü desteklemelidir. Anahtar servis türlerinin bilgilerini ayrıştırabilmeli ve aynı zamanda bu bilgileri işaretleyebilmelidir.

47. Ağ topolojisi üzerinde gereksinimlere göre bant genişliğini arttırmak amacıyla anahtar IEEE 802.3ad link aggregation protokolünü desteklemelidir. Böylece portlar belirli bir grup içerisinde toplanarak yüksek bant genişliği elde edilecektir.  Anahtar en az 128 adet link aggregation grubunu desteklemelidir ve her bir grubun içerisinde en az 8 adet gigabit port toplanabilmelidir. Oluşturulan grup içerisindeki portlardan herhangi birinin arızalanması durumunda grup bütünlüğü bozulmamalıdır.

48. Anahtar üzerinde IEEE 802.1d STP (Spanning-Tree Protocol) protokolü ve IEEE 802.1s MSTP (Multiple Spanning-Tree Protocol) protokolünü desteklemelidir. Anahtar ayrı vlanlar için vlan başına STP destekleyen PVST+ protokolünü desteklemelidir. Anahtar kullanıcı ve trunk  portlarında STP hesaplamalarını hızlandırabilmek amacıyla IEEE 802.1w RSTP (Rapid Spanning-Tree Protocol) protokolünü desteklemelidir. Anahtar üzerinde istenmeyen STP paketlerinin durdurulması amacıyla BPDU (Bridge Protocol Data Unit) paketlerinin istenilen arayüzden alınması, gönderilmesi ve filtrelenebilmesi desteklenmelidir. STP kök anahtarını koruyacak mekanizmalar anahtar üzerinde var olmaldır.

49. Anahtar jumbo frame özelliğini desteklemelidir. Desteklenen jumbo frame’lerin uzunluğu en az 9000 byte olmalıdır.

50. Anahtar kullanıcı portlarında broadcast fırtınalarını önleyerek ağ üzerindeki kullanılabilir bant genişliğini en uygun şekilde kullanabilmelidir. Anahtar üzerinde unicast ve multicast baskınlarına karşı koruma mekanizması olacaktır.

51. Anahtar üzerinde IEEE 802.1ab LLDP (Layer Link Discovery Protocol) desteği bulunacaktır.

52. Anahtar ağ üzerinde yedekli bir yapıyı destekleyebilmek amacıyla VRRP (Virtual Router Redundancy Protocol) ya da benzeri bir yedeklilik protokolünü destekleyebilmelidir.

53. Anahtar statik yönlendirme yapabilmelidir. Ripv1 , Ripv2 protokollerini desteklemelidir. Anahtar dinamik yönlendirme protokollerinden OSPF, IS-IS ve BGPv4 protokollerini  destekleyecektir. Ayrıca anahtar üzerinde politika bazlı yönlendirmeler de yapılabilmelidir.

54. Anahtar ağ üzerinde erişim kısıtlamaları yapabilmek amacıyla erişim denetim listelerini (Access Control List) desteklemelidir. Bu amaçla anahtar kullanıcıların belirli kaynaklara erişimini engelleyebilmelidir. Anahtar üzerinde yapılan erişim kısıtlamaları donanım bazlı olarak L2/L3/L4 seviyesinde olabilmelidir.

55. Anahtar donanımsal olarak ipv6 anahtarlama ve yönlendirme yeteneğine sahip olmalıdır. Anahtar ipv6 tabanlı dinamik yönlendirme protokollerinden RIPng, OSPFv3, MP-BGP, VRRPv3 protokolünü destekleyecektir.

56. Anahtar üzerinde ipv6 tabanlı politika bazlı yönlendirmeler desteklenmelidir.

57. Anahtar üzerinde ipv6 tabanlı erişim denetim listeleri (Access Control List)  ve servis önceliklendirme (Quality Of Services) protokolleri desteklenmelidir.

58. Anahtar ağ üzerindeki gereksiz trafiğin engellenmesi amacıyla multicast anahtarlama ve multicast yönlendirme yapabilmelidir. Bu amaçla anahtar IGMPv1/v2/v3 ve IGMP Snooping v1/v2/v3 standartlarını destekleyecektir. Anahtar ayrıca dinamik multicast yönlendirme RFC 2362 PIM-Sparse Mode, RFC 3973 PIM-Dense Mode ve RFC 3569 PIM-SSM (Source Specific Multicast) protokollerini destekleyebilmelidir.

59. Anahtar sanal yönlendirme ve iletim yapabilmek için VRF protokünü desteklemelidir ve ayrıca GRE (Generic Routing Encapsulation) özellikleri desteklenmelidir.

60. Anahtar kullanıcı portları üzerinde istenmeyen bir DHCP (Dynamic Host Configuration Protocol) sunucusunun bağlanmasını önlemek amacıyla DHCP snooping özelliğini desteklemelidir.

61. Anahtar üzerinde IGMP (Internet Group Management Protocol) protokolü filtreleme özelliği bulunmalıdır.IGMP v1/v2/v3 snooping desteklenmelidir. Bu sayede anahtar üzerinde multicast domain gruplarına üye olmayan kullanıcıların multicast yetkilendirmesi ve sınırlandırılması yapılabilecektir.

62. Anahtar ağ üzerinde kendisine bağlı olan diğer anahtarların öğrenme amacıyla neighbor discovery özelliğine sahip olamalıdır.

63. Anahtar üzerinde tüm portlar en az 4 adet RMON (Remote Monitoring) grubunu desteklemelidir.

64. Anahtar telnet, console portu ve  web arayüzü ile yönetilebilmelidir. Ayrıca anahtar üzerinde SNMPv1/v2/v3 (Simple Network Management Protocol) protokolü desteklenmelidir.

65. Anahtar üzerinde konsol port erişiminde farklı seviyelerde yetkilendirmeler tanımlanabilmelidir. Böylece anahtar üzerinde konfigürasyon yönetimi ve erişim kısmi yada tam yönetim şeklinde yapılabilecektir.

66. Anahtar ağ üzerindeki güvenliği sağlamak amacıyla, ağa bağlanan kullanıcılarının yetkilendirilmesi ve erişim politikalarının uygulanabilmesi için IEEE 802.1x protokolünü desteklemelidir. IEEE 802.1x protokolü ile bir yetkilendirme yazılımından ya da radius sunucusundan belirlenen izinler ile kullanıcı bazlı yetkilendirme yapılabilmelidir. Anahtar dinamik olarak VLAN yönlendirmelerini destekleyebilecektir.

67. Anahtarı yönetmek ve konfigüre etmek isteyen kullanıcılar Radius ve endüstri standartı TACACS+ protokolleri tarafından sorgulanabilmelidir.

68. Anahtar üzerinde gerektiğinde TFTP (Trivial File Transfer Protocol), FTP, SFTP, SCP protokolü ile yazılım dosyası güncellemesi, konfigürasyon dosyası saklanabilmesi yapılabilmelidir.

69. Anahtar ağ üzerindeki trafiği analiz edebilmek amacıyla port aynalama (mirroring) özelliğini desteklemelidir. Anahtar üzerinde belirlenen bir hedef portuna birden fazla kaynak portu aynalanabilmelidir (mirroring). Ayrıca poliçe bazlı aynalama yapılabilmelidir.

70. Anahtarın üzerindeki saat ve tarih bilgileri ağ üzerindeki diğer anahtarların saat ve tarih bilgileri ile senkron olabilmelidir. Bu amaçla anahtar NTP (Network Time Protocol) veya benzeri bir protokolü desteklemelidir.

71. Anahtar 19 inç Kabine montajı için gerekli parçaları ile sağlanacaktır.

72. Anahtarın en az 2 Gb flash, 2Gb hafızası olmalıdır.

73. Anahtarda SDN arayüzü olmalıdır ve Restful API,Openflow ve Openstack desteği bulunmalıdır.