

Załącznik nr 5 - Switch sieciowy – Specyfikacja

## Wymagania sprzętowe

1. 48 x porty Ethernet 10/100/1000Base-T, 4 x porty 10GE SFP+
2. 2 zasilacze redundantne 600W Hot Plug
3. Obsługa PoE+
4. Wydajność przekazywania: 125 Mpps
5. Przepustowość przełączania: 176 Gbps / 672 Gbps

## Wymagania funkcjonalne

1. **Tabela adresów MAC**
   1. Zgodność z normami IEEE 802.1d
   2. 64K wpisów adresów MAC
   3. Uczenie się i starzenie adresów MAC
   4. Statyczne, dynamiczne i czarne listy wpisów adresów MAC
   5. Filtrowanie pakietów na podstawie adresów MAC źródłowych
2. **VLAN**
   1. 4094 VLAN-ów
   2. VLAN gościa i VLAN głosowy
   3. GVRP (GARP VLAN Registration Protocol)
   4. MUX VLAN
   5. Przypisywanie VLAN-ów na podstawie adresów MAC, protokołów, podsieci IP, polityk i portów
   6. Mapowanie VLAN-ów
3. **Ochrona pętli Ethernet**
   1. Topologia pierścienia RRPP oraz wieloinstancjowy RRPP
   2. Topologia drzewa Smart Link i wieloinstancjowy Smart Link, zapewniające przełączanie ochronne na poziomie milisekund
   3. SEP (Smart Ethernet Protection)
   4. ERPS (G.8032)
   5. BFD (Bidirectional Forwarding Detection) dla OSPF, IS-IS, VRRP, i PIM
   6. STP (IEEE 802.1d), RSTP (IEEE 802.1w), i MSTP (IEEE 802.1s)
   7. Ochrona BPDU, ochrona root, oraz ochrona pętli
4. **MPLS**
   1. MPLS L3VPN
   2. MPLS L2VPN (VPWS/VPLS)
   3. MPLS-TE (Traffic Engineering)
   4. MPLS QoS
5. **Routing IP**
   1. Trasy statyczne, RIP v1/2, RIPng, OSPF, OSPFv3, IS-IS, IS-ISv6, BGP, BGP4+, ECMP, polityka routingu
   2. Do 32K wpisów FIBv4
   3. Do 8K wpisów FIBv6
6. **Interoperacyjność**
   1. VBST (VLAN-Based Spanning Tree), współpraca z PVST, PVST+ i RPVST
   2. LNP (Link-type Negotiation Protocol), podobny do DTP (Dynamic Trunking Protocol)
   3. VCMP (VLAN Central Management Protocol), podobny do VTP (VLAN Trunking Protocol)
7. **Funkcje IPv6**
   1. Do 8K wpisów ND
   2. PMTU (Path MTU Discovery)
   3. Ping IPv6, Tracert IPv6, oraz Telnet IPv6
   4. ACL na podstawie adresów źródłowych i docelowych IPv6, portów warstwy 4 lub typów protokołów
   5. Snooping MLDv1/v2 (Multicast Listener Discovery)
   6. Konfiguracja adresów IPv6 dla interfejsów, VRRP6, DHCPv6 oraz L3VPN
8. **Multicast**
   1. Snooping IGMP v1/v2/v3 oraz szybkie opuszczanie IGMP
   2. Przekazywanie multicastu w VLAN i replikacja multicastu między VLAN-ami
   3. Równoważenie obciążenia multicastu wśród portów członkowskich trunku
   4. Sterowalny multicast
   5. Statystyki ruchu multicastu na podstawie portów
   6. IGMP v1/v2/v3, PIM-SM, PIM-DM, i PIM-SSM
   7. MSDP (Multicast Source Discovery Protocol)
   8. MVPN (Multicast VPN)
9. **QoS/ACL**
   1. Ograniczenie prędkości w kierunku wejścia i wyjścia portu
   2. Przekierowanie pakietów
   3. Policing ruchu na podstawie portu oraz dwuwskaźnikowy model trójkolorowy CAR (Committed Access Rate)
   4. Osiem kolejek na port
   5. Algorytmy kolejkowania WDRR, SP i WDRR+SP
   6. WRED (Weighted Random Early Detection)
   7. Oznaczanie ponowne pól 802.1p oraz DSCP pakietów
   8. Filtrowanie pakietów na warstwach 2 do 4, filtrowanie nieprawidłowych ramek na podstawie źródłowych i docelowych adresów MAC, IP, numerów portów TCP/UDP, typu protokołu oraz identyfikatorów VLAN
   9. Ograniczenie szybkości oraz formowanie ruchu na podstawie kolejek portów
10. **Bezpieczeństwo**
    1. Hierarchiczne zarządzanie użytkownikami oraz ochrona hasłem
    2. Obrona przed atakami DoS, atakami ARP oraz atakami ICMP
    3. Wiązanie adresu IP, adresu MAC, numeru portu i identyfikatora VLAN
    4. Izolacja portów, ochrona portów i "Sticky MAC"
    5. MFF (MAC Forced Forwarding)
    6. Czarne listy adresów MAC
    7. Limit liczby nauczonych adresów MAC
    8. Autoryzacja IEEE 802.1x i limit liczby użytkowników na porcie
    9. AAA (Authentication, Authorization, Accounting), autoryzacja RADIUS oraz autoryzacja HWTACACS
    10. NAC (Network Admission Control)
    11. SSH w wersji 2.0
    12. HTTPS
    13. Ochrona CPU
    14. Czarna i biała lista
    15. Śledzenie źródeł ataku oraz karanie pakietów IPv6, takich jak ND, DHCPv6 oraz MLD
    16. Bezpieczny rozruch (Secure Boot)
    17. IPSec
    18. ECA (Encrypted Communication Analytics)
    19. Deception (Wykrywanie i izolowanie zagrożeń)
11. **Niezawodność**
    1. LACP (Link Aggregation Control Protocol)
    2. E-trunk
    3. Ethernet OAM (IEEE 802.3ah oraz IEEE 802.1ag)
    4. ITU-Y.1731
    5. DLDP (Device Link Detection Protocol)
    6. LLDP (Link Layer Discovery Protocol)
    7. BFD dla BGP, BFD dla IS-IS, BFD dla OSPF, BFD dla tras statycznych
12. **VXLAN**
    1. Bramki VXLAN warstw 2 i 3
    2. Bramki scentralizowane i rozproszone
    3. BGP-EVPN (BGP Extended VPN)
    4. Konfigurowalne poprzez protokół NETCONF
13. **Super Virtual Fabric (SVF)**
    1. Wspierana jest architektura klienta dwuwarstwowego
    2. Można włączyć snooping IGMP na przełącznikach dostępowych (AS), a także skonfigurować maksymalną liczbę użytkowników dostępu na porcie
    3. Przełączniki AS można konfigurować niezależnie
    4. Usługi nieobsługiwane przez szablony mogą być konfigurowane na nadrzędnym urządzeniu
    5. Dozwolone są urządzenia innych producentów pomiędzy nadrzędnym SVF a klientami
14. **iPCA**
    1. Bezpośrednie oznaczanie pakietów serwisowych w celu zbierania statystyk dotyczących liczby utraconych pakietów i wskaźnika strat pakietów w czasie rzeczywistym
    2. Zbieranie statystyk dotyczących liczby utraconych pakietów i wskaźnika strat pakietów na poziomie sieci i urządzeń
15. **TWAMP**
    1. Dwukierunkowy pomiar wydajności łączy IP
    2. Pomiar opóźnienia pakietów w obie strony, wskaźnika utraty pakietów w jedną stronę oraz jittera pakietów w jedną stronę
16. **Zarządzanie i utrzymanie**
    1. iStack, z możliwością złożenia stosu do 9 przełączników
    2. SNMP v1/v2c/v3
    3. RMON (Remote Monitoring)
    4. SAC (Smart Application Control)
    5. NMS (System Zarządzania Siecią) oparty na sieci Web
    6. Dzienniki systemowe i alarmy o różnych poziomach
    7. GVRP (GARP VLAN Registration Protocol)
    8. MUX VLAN
    9. NetStream
    10. Inteligentne O&M