VLAN TEXNOLOGIYASI VA UNING TARMOQ XAVFSIZLIGIDAGI RO'LI.

ТЕХНОЛОГИЯ VLAN И ЕЕ РОЛЬ В СЕТЕВОЙ БЕЗОПАСНОСТИ.

VLAN TECHNOLOGY AND ITS ROLE IN NETWORK SECURITY.

Ibragimov Shavkat Mamirovich
Farg'ona davlat universiteti, fizika-matematika fakulteti,
axborot texnologiyalari kafedrasi dotsenti.
shavkat70@bk.ru +998 90 530-18-04
http://orcid.org/0000-0001-7812-1898

Sohibova Charosxon Mansur qizi
Farg'ona davlat universiteti talabasi
charosxonsohibova@gmail.com

Annotatsiya: Ushbu maqolada VLAN (Virtual Local Area Network - Virtual Mahalliy Tarmoq) texnologiyasining mohiyati, turlari, ishlash printsiplari va tarmoq xavfsizligini ta'minlashdagi roli keng ko'lamda tahlil etilgan. Maqolada VLAN texnologiyasining paydo bo'lish tarixi, IEEE 802.1Q standarti asosida kadrlarni belgilash mexanizmi, kommutatorlarda VLAN sozlash usullari hamda tarmoqni segmentlash orqali xavfsizlikni oshirish imkoniyatlari ilmiy jihatdan yoritilgan. Shuningdek, VLAN ning an'anaviy tarmoq arxitekturasi bilan taqqoslanishi, Inter-VLAN routing tushunchasi, Access va Trunk portlarining farqlari hamda zamonaviy korporativ tarmoqlarda VLAN dan foydalanishning amaliy afzalliklari ko'rib chiqilgan. Tadqiqot natijalari shuni ko'rsatadiki, VLAN texnologiyasi tarmoqni mantiqiy segmentlash, broadcast domenlarini cheklash va ruxsatsiz kirishning oldini

olish orqali korporativ axborot tizimlarining xavfsizlik darajasini sezilarli darajada oshiradi.

Kalit so'zlar: VLAN, virtual mahalliy tarmoq, tarmoq xavfsizligi, IEEE 802.1Q, kommutator, trunk port, broadcast domeni, tarmoq segmentatsiyasi, Inter-VLAN routing, axborot xavfsizligi.

Аннотация: В данной статье подробно рассматриваются сущность, виды, принципы работы технологии VLAN (Virtual Local Area Network - виртуальная локальная сеть) и её роль в обеспечении сетевой безопасности. В статье научно освещены история возникновения технологии VLAN, механизм маркировки кадров на основе стандарта IEEE 802.1Q, методы настройки VLAN на коммутаторах, а также возможности повышения безопасности путём сегментирования сети. Кроме того, рассмотрены сравнение VLAN с традиционной сетевой архитектурой, концепция Inter-VLAN routing, различия между портами Access и Trunk, а также практические преимущества использования VLAN в современных корпоративных сетях. Результаты исследования показывают, что технология VLAN значительно повышает уровень безопасности корпоративных информационных систем за счёт логической сегментации сети, ограничения широковещательных доменов и предотвращения несанкционированного доступа.

Ключевые слова: VLAN, виртуальная локальная сеть, сетевая безопасность, IEEE 802.1Q, коммутатор, trunk-порт, широковещательный домен, сегментация сети, Inter-VLAN маршрутизация, информационная безопасность.

Annotation: This article provides a comprehensive analysis of the essence, types, operating principles of VLAN (Virtual Local Area Network) technology and its role in ensuring network security. The article scientifically covers the history of VLAN technology, the frame tagging mechanism based on the IEEE 802.1Q

standard, methods of configuring VLANs on switches, and the possibilities of improving security through network segmentation. Furthermore, the comparison of VLAN with traditional network architecture, the concept of Inter-VLAN routing, the differences between Access and Trunk ports, and the practical advantages of using VLAN in modern corporate networks are examined. The research results demonstrate that VLAN technology significantly increases the security level of corporate information systems through logical network segmentation, limiting broadcast domains, and preventing unauthorized access.

Keywords: VLAN, virtual local area network, network security, IEEE 802.1Q, switch, trunk port, broadcast domain, network segmentation, Inter-VLAN routing, information security.

KIRISH

Zamonaviy axborot texnologiyalari davrida korporativ va tashkiliy kompyuter tarmoqlari tobora murakkablashib, ularga ulangan qurilmalar soni tez sur'atlar bilan o'sib bormoqda. Bu holat, o'z navbatida, tarmoq xavfsizligini ta'minlash masalasini eng dolzarb muammolardan biriga aylantirmoqda. Yirik tashkilotlarda yuzlab, hatto minglab kompyuter va boshqa tarmoq qurilmalari bitta umumiy tarmoqqa ulangan bo'lib, ularni boshqarish, nazorat qilish va ruxsatsiz kirishdan himoya qilish katta amaliy ahamiyat kasb etadi.

An'anaviy mahalliy hisoblash tarmoqlarida (LAN - Local Area Network) barcha qurilmalar bitta broadcast domeniga kiradi. Bu shuni anglatadiki, tarmoqdagi bitta qurilma tomonidan yuborilgan broadcast xabari tarmoqdagi barcha boshqa qurilmalarga yetib boradi. Bunday holat bir tomondan tarmoq trafigining ortiqcha yuklanishiga, ikkinchi tomondan esa xavfsizlik nuqtayi nazaridan jiddiy muammolarga olib kelishi mumkin. Masalan, bir xodimning ish stantsiyasi boshqa bo'limlardagi maxfiy ma'lumotlarga nisbatan tarmoq paketlarini qabul qilishi korporativ axborot xavfsizligi uchun katta xavf tug'diradi.

Ushbu muammolarni hal etish maqsadida 1990-yillarning o'rtalarida VLAN (Virtual Local Area Network - Virtual Mahalliy Tarmoq) texnologiyasi ishlab chiqilgan va keng qo'llanila boshlagan. VLAN texnologiyasi yordamida fizik jihatdan bitta tarmoqqa ulangan qurilmalarni mantiqiy ravishda bir nechta alohida virtual tarmoqlarga bo'lish imkoni yaratildi. Bu esa tarmoq administratorlariga yagona fizik infratuzilma asosida bir nechta izolyatsiyalangan virtual tarmoq segmentlarini yaratish, boshqarish va nazorat qilish imkonini berdi.

Ushbu maqolaning maqsadi VLAN texnologiyasining ishlash prinsiplari, turlari va xususiyatlarini, shuningdek, uning tarmoq xavfsizligini ta'minlashdagi rolini ilmiy va amaliy nuqtayi nazardan tahlil etishdan iborat. Maqolada IEEE 802.1Q standarti asosida VLAN ni amalga oshirish mexanizmlari, Access va Trunk portlarining farqlari, Inter-VLAN routing tushunchasi va VLAN ni joriy etishning xavfsizlikdagi afzalliklari batafsil ko'rib chiqiladi. Tadqiqotning axborot bazasini mashhur tarmoq muhandisligi sohasidagi darsliklar, ilmiy maqolalar va rasmiy standartlar tashkil etadi.

ADABIYOTLAR TAHLILI VA USULLAR

VLAN texnologiyasining paydo bo'lish tarixi 1980-yillarning oxiri va 1990-yillarning boshlariga to'g'ri keladi. Ushbu davrda korporativ tarmoqlar tobora murakkablashib, an'anaviy tarmoq arxitekturasi ko'plab cheklovlarini ko'rsata boshladi. Andrew S. Tanenbaum o'zining "Computer Networks" asarida ta'kidlaganidek: "Katta tarmoqlarda broadcast trafigining nazoratdan chiqishi tarmoq unumdorligini keskin pasaytirishi mumkin" (Tanenbaum, 2011, 364-bet).

Dastlabki VLAN yechimlari turli ishlab chiqaruvchilar (Cisco, 3Com, Bay Networks) tomonidan o'z xususiy protokollari asosida taqdim etilgan. Biroq bu holat o'zaro muvofiqlashish (interoperability) muammolarini keltirib chiqardi. Ushbu muammoni bartaraf etish maqsadida IEEE (Institute of Electrical and Electronics Engineers) 1998-yilda 802.1Q standarti - VLAN Tagging (VLAN belgilash) protokolini rasman tasdiqladi. Mazkur standart bugungi kunda ham VLAN

texnologiyasining asosiy mezoni hisoblanadi va barcha yetakchi tarmoq qurilmalari ishlab chiqaruvchilari tomonidan qo'llaniladi.

Wendell Odom ning "CCNA 200-301 Official Cert Guide" asarida ta'kidlanishicha, 802.1Q standarti Ethernet kadrlarini VLAN identifikatori (VID - VLAN ID) bilan belgilash mexanizmini standartlashtirdi va bu 1-dan 4094-gacha bo'lgan VLAN identifikatorlari orqali tarmoqlarni mantiqiy ajratish imkonini berdi (Odom, 2020, 192-bet).

VLAN ning Mohiyati va Ishlash Printsiplari

VLAN - bu fizik tarmoq topologiyasidan qat'iy nazar, mantiqiy jihatdan ajratilgan tarmoq segmentidir. Klassik ta'rifga ko'ra, VLAN - kommutatsiyalangan tarmoqdagi bir yoki bir nechta kommutatorlardagi portlarning shunday mantiqiy guruhiki, ulardagi qurilmalar bir broadcast domeniga mansub bo'lib, o'zaro bevosita Layer 2 (kanal darajasi) orqali muloqot qila oladi, boshqa VLAN lardan esa mantiqiy jihatdan izolyatsiyalangan.

James F. Kurose va Keith W. Ross o'zlarining "Computer Networking: A Top-Down Approach" asarida VLAN ning asosiy afzalliklarini quyidagicha izohlaydi:

Tarmoq izolyatsiyasi	Broadcast domenlarining cheklanishi	Moslashuvchanlik
Turli VLAN lardagi qurilmalar bir-biridan mantiqiy jihatdan ajratilgan bo'lib, ular orasidagi muloqot faqat Layer 3 qurilmasi (router yoki Layer 3 kommutator) orqali amalga oshirilishi mumkin.	Har bir VLAN o'zining alohida broadcast domeniga ega, bu esa tarmoq trafigini sezilarli darajada kamaytiradi.	Qurilmalarni fizik ko'chirmasdan, faqat port konfiguratsiyasini o'zgartirish orqali ularni boshqa VLAN ga o'tkazish mumkin

VLAN ning ishlash printsipini quyidagicha izohlash mumkin: kommutator har bir portiga VLAN identifikatori (VLAN ID) biriktiriladi. Biror port orqali kommutatorga yetib keladigan Ethernet kadri u tegishli VLAN bo'yicha ishlanadi va faqat o'sha VLANga tegishli portlarga yo'naltiriladi. Boshqa VLAN portlariga kadr yo'naltirilmaydi, bu esa mantiqiy izolyatsiyani ta'minlaydi.

IEEE 802.1Q standarti VLAN texnologiyasining texnik asosini tashkil etadi. Mazkur standart Ethernet kadrining sarlavhasiga (header) qo'shimcha 4 baytli maydon - 802.1Q tegi (tag) - qo'shish mexanizmini belgilaydi. Ushbu teg ikki asosiy qismdan iborat:

1. TPID (Tag Protocol Identifier) - 2 baytli maydon, 0x8100 qiymati bilan, bu kadrda 802.1Q tegi mavjudligini bildiradi.
2. TCI (Tag Control Information) - 2 baytli maydon, o'z navbatida quyidagilarni o'z ichiga oladi:
3. PCP (Priority Code Point) - 3 bit, IEEE 802.1p standarti bo'yicha xizmat sifatini (QoS) belgilash uchun.
4. DEI (Drop Eligible Indicator) - 1 bit, tarmoq yuklanishi ortgan holda kadrni tashlab yuborish mumkinligini bildiradi.
5. VID (VLAN Identifier) - 12 bit, VLAN identifikatorini ko'rsatadi. 12 bitlik maydon 0 dan 4095 gacha raqamlash imkonini beradi, ammo 0 va 4095 raqamlari maxsus maqsadlarga ajratilgan. Shunday qilib, nazariy jihatdan 4094 ta alohida VLAN yaratish mumkin.

Wendell Odom ta'kidlaganidek, ushbu belgilash (tagging) jarayoni trunk port orqali uzatiladigan kadrlarga nisbatan amalga oshiriladi. Access portlardan keladigan kadrlar esa kommutator tomonidan tegishli VLAN ID bilan belgilanadi va trunk portlar orqali uzatish jarayonida teglar saqlanadi, access portlardan chiqishda esa teglar olib tashlanadi (tarmoq muhandisligi adabiyotida VLAN larning bir necha turi ajratib ko'rsatiladi)

Port asosidagi VLAN (Port-Based VLAN) - eng keng tarqalgan va oddiy VLAN turi bo'lib, kommutator portiga tegishli VLAN ID biriktiriladi. Port orqali tarmoqqa ulangan qurilma avtomatik ravishda o'sha portga biriktirilgan VLANga mansub bo'ladi. Bu tur korporativ tarmoqlarda eng ko'p qo'llaniladi.

MAC-manzil asosidagi VLAN (MAC-Based VLAN) - ushbu turda VLAN a'zoligi qurilmaning MAC-manziliga asoslanadi. Qurilma qaysi portga ulanmasin, uning MAC-manzili bo'yicha u tegishli VLANga kiritiladi. Bu usul ko'chma qurilmalar (noutbuklar, planshetlar) uchun qulay, ammo boshqaruv nuqtayi nazaridan murakkabrok.

Protokol asosidagi VLAN (Protocol-Based VLAN) - tarmoq trafigining protokol turiga (IPv4, IPv6, IPX va h.k.) ko'ra VLAN larga bo'linish amalga oshiriladi. Ushbu tur kamdan-kam hollarda qo'llaniladi.

Dinamik VLAN - Cisco's Dynamic Trunking Protocol (DTP) yoki VLAN Membership Policy Server (VMPS) kabi mexanizmlar yordamida qurilmalarni avtomatik ravishda VLANlarga kiritish imkoni mavjud. Bu tur yirik tarmoqlarda boshqaruvni osonlashtiradi.

VLAN texnologiyasida kommutator portlari asosan ikki rejimda ishlaydi: Access va Trunk. Access Port (Kirish porti) - faqat bitta VLANga tegishli portdir. Odatda yakuniy qurilmalar (kompyuterlar, printerlar, IP-telefonlar) ulanadigan portlar access rejimida konfiguratsiya qilinadi. Access portdan o'tadigan kadrlarda 802.1Q tegi bo'lmaydi - kommutator kerakli tegni o'zi qo'shadi yoki olib tashlaydi. Trunk Port (Magistral port) - bir nechta VLAN trafigini bir vaqtda uzatish qobiliyatiga ega port. Asosan ikki kommutator yoki kommutator bilan router o'rtasidagi ulanishlarda qo'llaniladi. Trunk port orqali o'tadigan kadrlarda 802.1Q tegi mavjud bo'lib, u qaysi VLANga tegishliligini ko'rsatadi.

Todd Lammle o'zining "CompTIA Network+ Study Guide" asarida ta'kidlaganidek, trunk portlar yirik tarmoqlarda VLAN trafigini kommutatorlar orasida samarali uzatishning asosiy vositasi hisoblanadi. Trunk portlarda "native

VLAN" tushunchasi ham mavjud bo'lib, u belgilanmagan kadrlarning qaysi VLANga mansub bo'lishini belgilaydi va odatda VLAN 1 bo'ladi (Lammle, 2019, 278-bet).

MUHOKAMA

VLAN lar o'zaro izolyatsiyalangan bo'lganligi sababli, turli VLANdagi qurilmalar orasida muloqot o'rnatish uchun Layer 3 qurilmasi - router yoki Layer 3 kommutator - talab etiladi. Bu jarayon Inter-VLAN routing deb nomlanadi. Inter-VLAN routing ning uchta asosiy usuli mavjud. Router on a Stick (Tayoqchali router) - bitta router porti trunk rejimida kommutatorga ulanib, har bir VLAN uchun alohida mantiqiy subinterface (pastki interfeys) yaratiladi. Har bir subinterfeys o'z IP-manzili va VLAN identifikatori bilan konfiguratsiya qilinadi. Bu usul oddiy va arzon, ammo katta trafik yuklamalarida router porti to'siq (bottleneck) bo'lib qolishi mumkin. Alohida router interfeyslari orqali - har bir VLAN uchun routerda alohida fizik interfeys ishlatiladi. Bu usul yuqori unumdorlik ta'minlasa-da, katta tarmoqlarda interfeys sonining yetishmasligi muammo tug'dirishi mumkin. Layer 3 kommutator orqali - zamonaviy korporativ tarmoqlarda eng ko'p qo'llaniladigan usul. Layer 3 kommutatorlar ham kommutatsiya, ham marshrutlash funksiyalarini birlashtirib, SVI (Switched Virtual Interface) orqali VLANlar orasida yuqori tezlikda marshrutlash amalga oshiradi. Odom ta'kidlaganidek, Layer 3 kommutatorlar hardwarebased routing imkoniyati tufayli an'anaviy routerlarga nisbatan ancha yuqori unumdorlikni ta'minlaydi.

VLAN ning Tarmoq Xavfsizligidagi Roli

VLAN texnologiyasining tarmoq xavfsizligini ta'minlashdagi roli ko'p qirrali bo'lib, quyidagi asosiy jihatlarni o'z ichiga oladi:

Tarmoq segmentatsiyasi va izolyatsiya - VLAN yordamida tarmoqni segmentlash xavfsizlikning asosiy tamoyillaridan biri bo'lgan "eng kam imtiyoz" (Principle of Least Privilege) prinsipini tarmoq darajasida amalga oshirishga imkon beradi. Masalan, moliya bo'limi, IT xizmati, mehmonlar va serverlar uchun alohida

VLANlar yaratilganda, agar bitta segmentdagi qurilma virusga yoki tarmoq hujumiga duchor bo'lsa, muammo boshqa VLANlarga tarqalishi sezilarli darajada cheklanadi. William Stallings "Cryptography and Network Security" asarida ta'kidlaganidek: "Tarmoq segmentatsiyasi - ko'plab xavfsizlik muammolariga nisbatan samarali dastlabki chiziq (first line of defense) hisoblanadi".

Broadcast hujumlaridan himoya - broadcast domeni qanchalik katta bo'lsa, tarmoq trafigining ko'p qismi broadcast xabarlari bilan band bo'ladi va bu holat Smurf Attack, ARP Flooding kabi hujumlar uchun qulay muhit yaratadi. VLAN yordamida broadcast domenlar kichik segmentlarga bo'linadi va shu tariqa ushbu turdagi hujumlarning tarqalishi cheklanadi.

VLAN hopping hujumlariga qarshi choralar - VLAN ning xavfsizlikdagi asosiy zaifliklaridan biri VLAN Hopping hujumidir. Bu hujumda tajovuzkor bir VLANdan boshqa VLANga ruxsatsiz kirish imkoniyatiga ega bo'lishga harakat qiladi. Ushbu hujumning ikki asosiy usuli mavjud:

1. Switch Spoofing: Tajovuzkor o'z kompyuterini kommutator sifatida taqdim etib, trunk ulanishni o'rnatishga urinadi va shu orqali barcha VLAN trafiklariga kirish imkonini olishga intiladi.
2. Double Tagging (Ikki tomonlama belgilash): Tajovuzkor paketga ikkita 802.1Q tegi qo'yib, birinchi teg native VLANga mos kelmasa, kommutator ikkinchi tegni ko'radi va paket boshqa VLANga yo'naltiriladi.

Ushbu hujumlardan himoyalanish uchun tarmoq mutaxassislari quyidagi choralarni tavsiya etadi:

1. Foydalanilmayotgan portlarni o'chirib qo'yish yoki ularni foydalanilmaydigan (unused) VLANga biriktirish.
2. Native VLAN ni standart VLAN 1 dan farqli VLANga o'zgartirish.
3. DTP (Dynamic Trunking Protocol) ni foydalanilmaydigan portlarda o'chirish.
4. Access portlarni manual ravishda "switchport mode access" buyrug'i bilan konfiguratsiya qilish.

VLAN texnologiyasi kirish nazorati ro'yxatlari (ACL - Access Control List) bilan birga ishlatilganda tarmoq xavfsizligi yanada mustahkamlanadi. VLAN SVIlariga yoki router interfeyslariga qo'llaniladigan ACLlar VLANlar orasidagi trafikni granular darajada nazorat qilish imkonini beradi. Masalan, moliya VLANidan faqat ma'lum IP-manzillarga yoki portlarga kirish ruxsat berilishi mumkin. Zamonaviy korporativ tarmoqlarda tashqi mehmonlar, pudratchilar (contractors) yoki shaxsiy qurilmalar (BYOD - Bring Your Own Device) uchun alohida VLAN yaratish keng amaliyotga kirib kelgan. Bu usul mehmonlar Internetga kirish imkoniyatiga ega bo'lishini ta'minlaydi, ammo ularni korporativ ichki tarmoq resurslaridan izolyatsiyalaydi. Bunday yondashuv APT (Advanced Persistent Threat) hujumlarining tarmoq ichida tarqalish xavfini sezilarli darajada kamaytiradi. VLAN texnologiyasi zamonaviy korporativ xavfsizlik arxitekturasida alohida emas, balki boshqa xavfsizlik vositalari bilan birgalikda ishlaydi:

VLAN va Firewall - zo'r-bazo'r tarmoq arxitekturalarida har bir VLAN trafigi firewall orqali o'tkaziladi. Bu DMZ (Demilitarized Zone) konsepsiyasini amalga oshirishda muhim rol o'ynaydi. Masalan, serverlar VLANi va foydalanuvchi VLANi o'rtasidagi muloqot firewall qoidalari bilan nazorat qilinadi.

VLAN va 802.1X Port autentifikatsiyasi - IEEE 802.1X standarti port asosidagi tarmoqqa kirish nazoratini (Network Access Control) ta'minlab, foydalanuvchi yoki qurilmani autentifikatsiya qilmasdan tarmoqqa kirishini bloklaydigan mexanizm hisoblanadi. 802.1X va VLAN texnologiyalarining integratsiyasi dinamik VLAN biriktirishni (Dynamic VLAN Assignment) amalga oshirish imkonini beradi: RADIUS server autentifikatsiya natijasiga ko'ra foydalanuvchini avtomatik ravishda tegishli VLANga kiritadi.

VLAN va Network Monitoring VLAN - segmentatsiyasi tarmoq monitoringini ham osonlashtiradi. Har bir VLAN alohida kuzatilishi mumkin bo'lib, anomal trafik naqshlari tezroq aniqlanadi. SIEM (Security Information and Event

Management) tizimlari va IDS/IPS (Intrusion Detection/Prevention Systems) lar VLAN asosida sozlanganda aniqlik va samaradorlik oshadi.

NATIJALAR

VLAN (Virtual Local Area Network) texnologiyasi zamonaviy kompyuter tarmoqlarida nafaqat tarmoqni mantiqiy segmentlarga ajratish, balki uning xavfsizligi, boshqaruv qulayligi va samaradorligini oshirishda ham muhim ahamiyat kasb etadi. VLAN yordamida broadcast domenlarni kichraytirish orqali tarmoqdagi ortiqcha trafik kamayadi, natijada tarmoq unumdorligi va ishlash tezligi oshadi. Shu bilan birga, turli bo‘limlar va foydalanuvchilarni alohida segmentlarga ajratish orqali tarmoq resurslari ustidan nazorat kuchayadi hamda xavfsizlik darajasi sezilarli ravishda yaxshilanadi. Inter-VLAN routing texnologiyalari VLANlar o‘rtasida muloqotni tashkil etish imkonini beradi. Router on a Stick, alohida router interfeyslari va Layer 3 kommutator orqali marshrutlash usullari turli tarmoq ehtiyojlariga mos ravishda qo‘llaniladi. Ayniqsa, Layer 3 kommutatorlar yuqori tezlik va samaradorlikni ta’minlagani sababli korporativ tarmoqlarda keng qo‘llanilmoqda. Tahlillar shuni ko‘rsatadiki, VLAN texnologiyasi tarmoq xavfsizligining muhim elementi hisoblanadi. VLAN segmentatsiyasi zararli trafik va hujumlarning butun tarmoqqa tarqalishini cheklaydi, broadcast asosidagi hujumlar xavfini kamaytiradi hamda ACL, firewall va 802.1X kabi xavfsizlik texnologiyalari bilan integratsiyalashganda yanada kuchli himoya mexanizmini yaratadi. Shu bilan birga, VLAN Hopping kabi tahdidlarga qarshi to‘g‘ri konfiguratsiya va xavfsizlik choralarini qo‘llash zarur ekanligi aniqlandi.

XULOSA

Ushbu maqolada VLAN texnologiyasining mohiyati, ishlash prinsiplari, turlari va tarmoq xavfsizligidagi roli ilmiy jihatdan keng tahlil etildi. Amalga oshirilgan tadqiqot natijasida quyidagi asosiy xulosalar chiqarildi:

VLAN texnologiyasi zamonaviy korporativ tarmoqlarda xavfsizlik arxitekturasining ajralmas qismiga aylangan bo'lib, u fizik tarmoqlarni mantiqiy

segmentlarga bo'lish orqali xavfsizlikni ta'minlashning eng samarali usullaridan biri hisoblanadi. IEEE 802.1Q standarti ushbu texnologiyaning barcha asosiy ishlab chiqaruvchilar tomonidan qo'llab-quvvatlanadigan universal asosini tashkil etadi. VLAN broadcast domenlarini cheklash orqali tarmoq trafigini optimallashtiradi va shu bilan birga tarmoq hujumlarining tarqalish maydonini keskin qisqartiradi. Moliya bo'limi, IT xizmati, serverlar va mehmonlar kabi turli xavfsizlik darajalaridagi segmentlarni ajratish orqali "eng kam imtiyoz" prinsipini tarmoq darajasida amalga oshirish imkoni yaratiladi.

FOYDALANILGAN ADABIYOTLAR

1. Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th ed.). Prentice Hall. - 364, 381–395-betlar.
2. Kurose, J. F., & Ross, K. W. (2017). Computer Networking: A Top-Down Approach (7th ed.). Pearson. - 493–510-betlar.
3. Odom, W. (2020). CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. - 185–225-betlar.
4. Lammle, T. (2019). CompTIA Network+ Study Guide: Exam N10-007 (4th ed.). Sybex / Wiley. - 265–290-betlar.
5. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson. - 735–755-betlar.
6. Forouzan, B. A. (2013). Data Communications and Networking (5th ed.). McGraw-Hill. - 462–478-betlar.
7. Doyle, J., & Carroll, J. (2005). Routing TCP/IP, Volume I (2nd ed.). Cisco Press. - 52–75-betlar.
8. Cisco Systems. (2020). Cisco IOS LAN Switching Configuration Guide. Cisco Systems Inc. - 12.2 nashr.

9. IEEE. (2018). IEEE Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks (IEEE 802.1Q). Institute of Electrical and Electronics Engineers.
10. Comer, D. E. (2015). Computer Networks and Internets (6th ed.). Pearson. - 210–228-betlar.