ISNN 3030-3907

2026
MAY
ISSUE - 5
VOLUME - 4

DEVELOPMENT OF SCIENCE

scientific journal



Development of science

Ilmiy jurnal

MAY 2026
Issue - 5, VOLUME - 4

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

KORXONA TARMOQLARIDA VLAN SEGMENTATSIYASI ORQALI XAVFSIZLIKNI OSHIRISH USULLARI

Ro‘zimov Javlonbek Sabirjon o‘g‘li
URDU Axborot xavfsizligi kafedrasi o‘qituvchisi
Tel: +998-91-999-96-60
E-mail: rjavlonj6@gmail.com

Annotatsiya. Ushbu maqolada korxona tarmoqlarida VLAN (Virtual Local Area Network) texnologiyasi yordamida tarmoq segmentatsiyasini amalga oshirish va uning axborot xavfsizligini ta’minlashdagi ahamiyati tahlil qilinadi. VLAN texnologiyasining broadcast trafikni kamaytirish, foydalanuvchilarni mantiqiy segmentlarga ajratish hamda ichki tarmoq hujumlarini oldini olishdagi roli ko‘rib chiqiladi. Shuningdek, VLAN hopping, switch spoofing va noto‘g‘ri konfiguratsiya kabi xavfsizlik tahdidlari hamda ularni bartaraf etish usullari tahlil etiladi. Tadqiqot davomida VLAN segmentatsiyasining korxona tarmoqlarida xavfsizlikni oshirishdagi samaradorligi yoritilgan.

Kalit so‘zlar. VLAN, tarmoq xavfsizligi, segmentatsiya, VLAN hopping, switch spoofing, trunk port, Cisco switch, axborot xavfsizligi, korxona tarmoqlari.

Аннотация. В данной статье анализируется роль технологии VLAN (Virtual Local Area Network) в сегментации корпоративных сетей и обеспечении информационной безопасности. Рассматриваются возможности VLAN по снижению широковещательного трафика, логическому разделению пользователей и предотвращению внутренних сетевых атак. Также исследуются угрозы безопасности, такие как VLAN hopping, switch spoofing и ошибки конфигурации, а также методы их предотвращения. В ходе исследования показана эффективность VLAN-сегментации в повышении уровня безопасности корпоративных сетей.

Ключевые слова. VLAN, сетевая безопасность, сегментация, VLAN hopping, switch spoofing, trunk port, Cisco switch, информационная безопасность, корпоративные сети.

Abstract. This article analyzes the role of VLAN (Virtual Local Area Network) technology in enterprise network segmentation and information security enhancement. The study examines the effectiveness of VLAN technology in reducing broadcast traffic, logically separating users, and preventing internal network attacks. Security threats such as VLAN hopping, switch spoofing, and configuration vulnerabilities are also discussed along with protection methods. The research demonstrates the efficiency of VLAN segmentation in improving the security of enterprise networks.

Keywords. VLAN, network security, segmentation, VLAN hopping, switch spoofing, trunk port, Cisco switch, information security, enterprise networks.

KIRISH.

Zamonaviy axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida korxona tarmoqlarining hajmi, murakkabligi va ularga ulanayotgan foydalanuvchilar soni keskin ortib bormoqda. Korxonalarda turli bo‘limlar, serverlar, IoT qurilmalar, simsiz tarmoqlar hamda bulutli xizmatlarning yagona infratuzilmada ishlashi tarmoq xavfsizligini ta’minlashni yanada murakkablashtirmoqda. Ayniqsa, ichki tarmoq orqali amalga oshiriladigan ruxsatsiz kirishlar, ma’lumotlarning sizib chiqishi, broadcast trafikning ortishi va lateral movement turidagi hujumlar korxona axborot xavfsizligi uchun jiddiy tahdid hisoblanadi.

An’anaviy lokal tarmoqlarda barcha foydalanuvchilarning yagona broadcast domenida ishlashi tarmoq resurslaridan foydalanish samaradorligini pasaytiradi hamda xavfsizlik muammolarini yuzaga keltiradi. Bunday holatda bir foydalanuvchi tomonidan amalga oshirilgan zararli faoliyat boshqa segmentlarga ham tez tarqalishi mumkin. Shu sababli tarmoqlarni mantiqiy segmentlarga ajratish orqali xavfsizlikni oshirish zarurati paydo bo‘ladi. Ushbu vazifani bajarishda VLAN (Virtual Local Area Network) texnologiyasi muhim vositalardan biri hisoblanadi.

VLAN texnologiyasi fizik jihatdan bitta switch yoki bir nechta switch qurilmalarida ishlovchi foydalanuvchilarni mantiqiy guruhlarga ajratish imkonini beradi. Natijada tarmoqdagi broadcast trafik kamayadi, foydalanuvchilar o‘rtasidagi kirishlar cheklanadi hamda ma’lumot almashinuvi nazorat qilinadi. VLAN segmentatsiyasi yordamida korxona bo‘limlari alohida tarmoq segmentlariga ajratilib, maxfiy ma’lumotlarning himoyalanish darajasi oshiriladi.

Shuningdek, VLAN texnologiyasi xavfsizlikni oshirish bilan birga ayrim zaifliklarga ham ega. Xususan, VLAN hopping, switch spoofing, double tagging kabi hujumlar noto‘g‘ri sozlangan tarmoqlarda jiddiy xavf tug‘dirishi mumkin. Shu sababli VLAN infratuzilmasini xavfsiz tashkil etish va himoya mexanizmlarini to‘g‘ri qo‘llash muhim ahamiyat kasb etadi.

I. VLAN texnologiyasining nazariy asoslari

VLAN (Virtual Local Area Network) — bu lokal tarmoqni mantiqiy segmentlarga ajratish texnologiyasi hisoblanadi. VLAN texnologiyasi IEEE 802.1Q standarti asosida ishlaydi va Ethernet freymlariga maxsus identifikator qo‘shish orqali paketlarning tegishli VLAN’ga mansubligini aniqlaydi.

Har bir VLAN alohida broadcast domen sifatida ishlaydi. Bu esa broadcast trafikni kamaytiradi va tarmoq unumdorligini oshiradi. Switch portlari access va trunk rejimlarda ishlashi mumkin. Access port odatda bitta VLAN uchun ishlatiladi, trunk port esa bir nechta VLAN trafiklarini uzatadi.

ISSN 3030-3907

Korxona tarmoqlarida VLAN segmentatsiyasi ko‘pincha bo‘limlar asosida tashkil qilinadi. Masalan:

VLAN 10 — Accounting

VLAN 20 — HR

VLAN 30 — IT bo‘limi

VLAN 40 — Mehmonlar tarmog‘i

Bunday segmentatsiya orqali foydalanuvchilarning o‘zaro aloqalari nazorat qilinadi va maxfiy ma’lumotlarga ruxsatsiz kirish ehtimoli kamayadi.

II. VLAN segmentatsiyasining xavfsizlikdagi ahamiyati

Korxona tarmoqlarida axborot xavfsizligini ta’minlashning muhim usullaridan biri tarmoq segmentatsiyasini to‘g‘ri tashkil qilish hisoblanadi. Tarmoq segmentatsiyasi foydalanuvchilar va qurilmalarni alohida mantiqiy guruhlarga ajratish orqali trafik oqimini nazorat qilish imkonini beradi.

VLAN segmentatsiyasining asosiy xavfsizlik afzalliklaridan biri foydalanuvchilarni izolatsiya qilishdir. Har bir VLAN mustaqil broadcast domen sifatida ishlaydi va boshqa segmentlardan ajratiladi. Bu esa maxfiy ma’lumotlarni himoyalashda muhim rol o‘ynaydi.

VLAN segmentatsiyasi ichki tahdidlarni kamaytirishda ham muhim hisoblanadi. Agar barcha qurilmalar bitta segmentda joylashgan bo‘lsa, hujumchi tarmoq ichida erkin harakatlanishi mumkin. VLAN yordamida esa lateral movement cheklanadi va hujum faqat ma’lum segment doirasida qoladi.

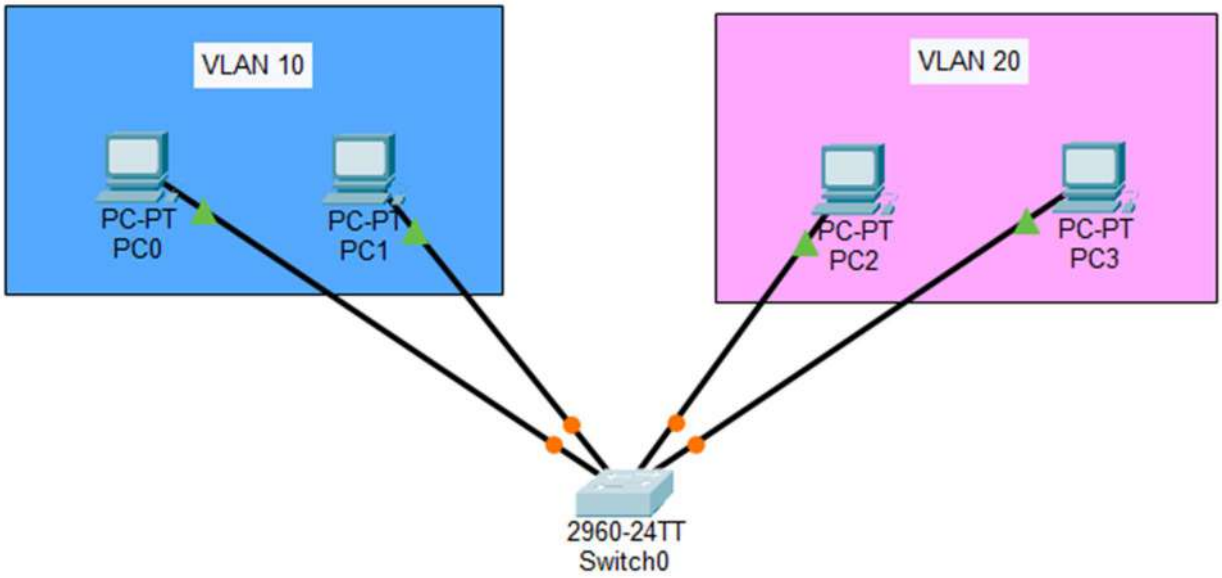
III. Amaliy tajriba

Mazkur amaliy tajriba Cisco Packet Tracer simulyatsiya muhiti asosida amalga oshirildi. Tajribaning asosiy maqsadi korxona tarmoqlarida VLAN segmentatsiyasi orqali xavfsizlikni oshirish, VLAN hopping kabi xavfsizlik tahdidlarini modellashtirish hamda himoya konfiguratsiyalarini qo‘llashdan iborat bo‘ldi. Tajriba davomida Cisco 2960 switch qurilmasi va to‘rtta ishchi stansiyadan foydalanildi.

3.1. VLAN segmentatsiyasini yaratish

Dastlab tarmoq ikki alohida segmentga ajratildi: VLAN 10 (Accounting) va VLAN 20 (HR). Har bir VLAN uchun alohida portlar biriktirildi va foydalanuvchi qurilmalari mos IP manzillar bilan sozlandi. Natijada tarmoqning broadcast domenlari mantiqiy ravishda ajratildi.

ISSN 3030-3907



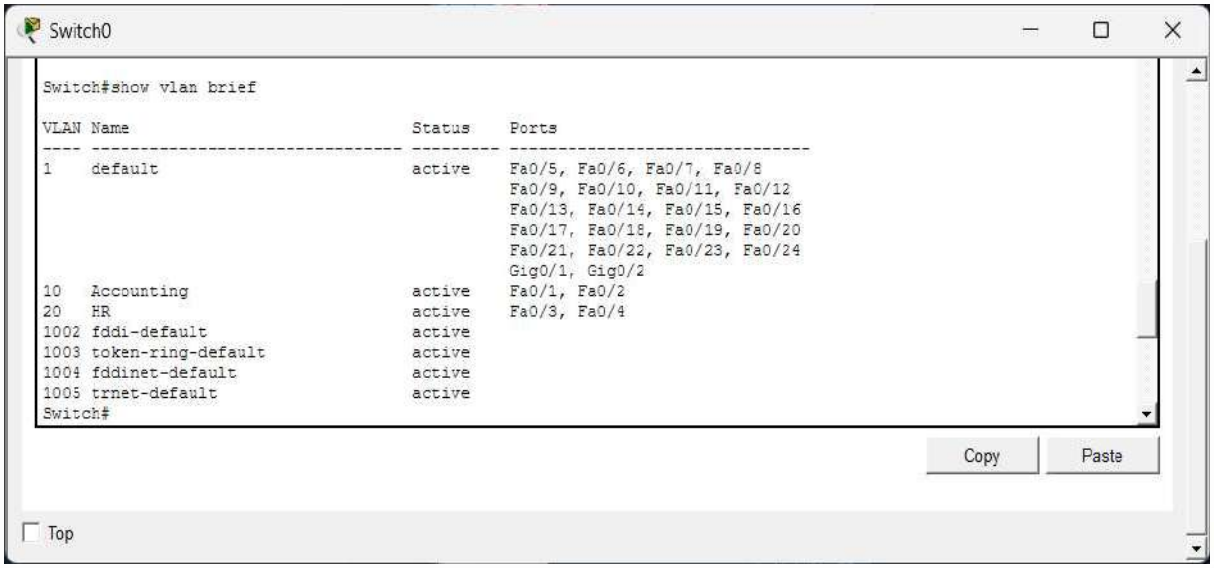
1-rasm. VLAN segmentatsiyasi asosida qurilgan topologiya.

Switch qurilmasida quyidagi VLAN konfiguratsiyasi amalga oshirildi:

VLAN 10 → Fa0/1, Fa0/2

VLAN 20 → Fa0/3, Fa0/4

VLAN 999 → Native-Blackhole

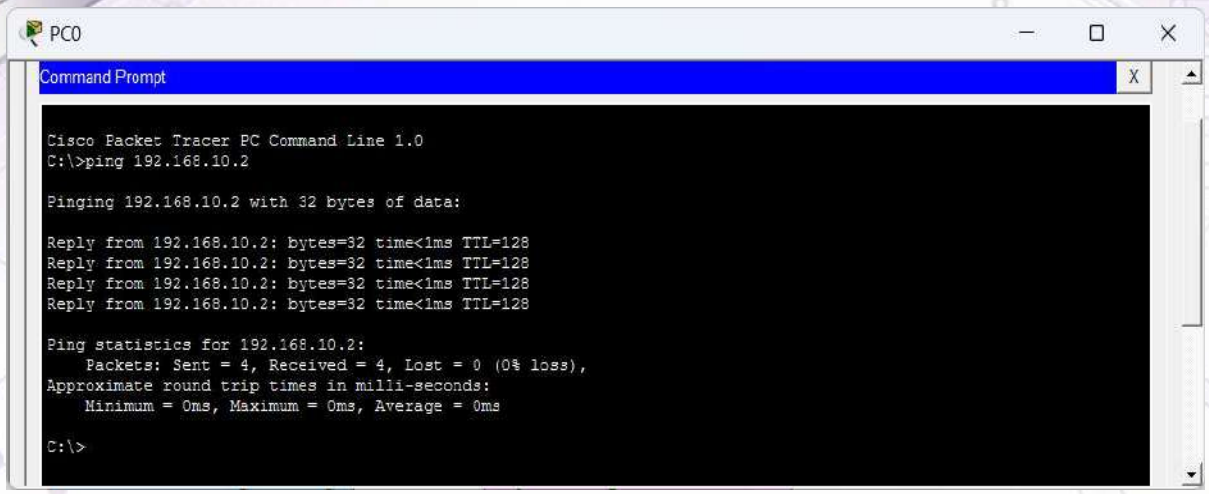


2-rasm. Switch qurilmasida yaratilgan VLAN konfiguratsiyasi va portlarning VLAN'larga biriktirilishi.

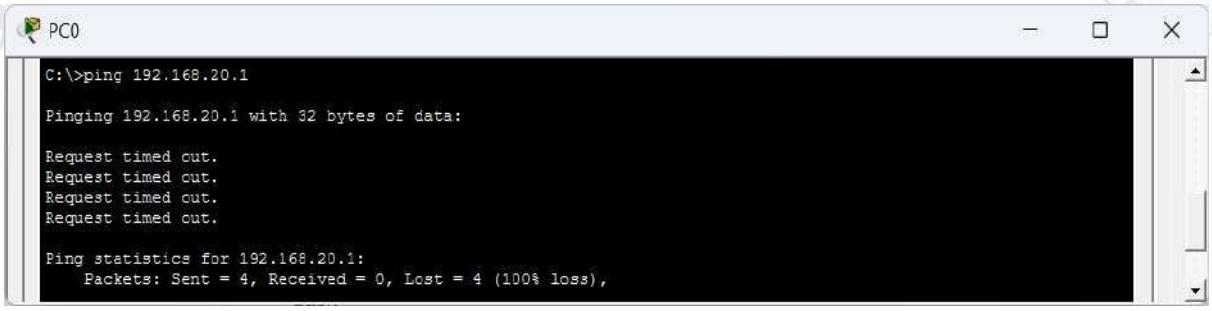
3.2. VLAN ichidagi va VLANlararo trafikni tahlil qilish

Tarmoq segmentatsiyasi samaradorligini tekshirish maqsadida ping sinovlari o‘tkazildi. VLAN 10 ichidagi qurilmalar o‘zaro muvaffaqiyatli aloqa o‘rnata oldi. Biroq VLAN 10 dan VLAN 20 ga yuborilgan ICMP paketlari bloklandi.

ISSN 3030-3907



3-rasm. VLAN 10 ichidagi muvaffaqiyatli ping natijasi.



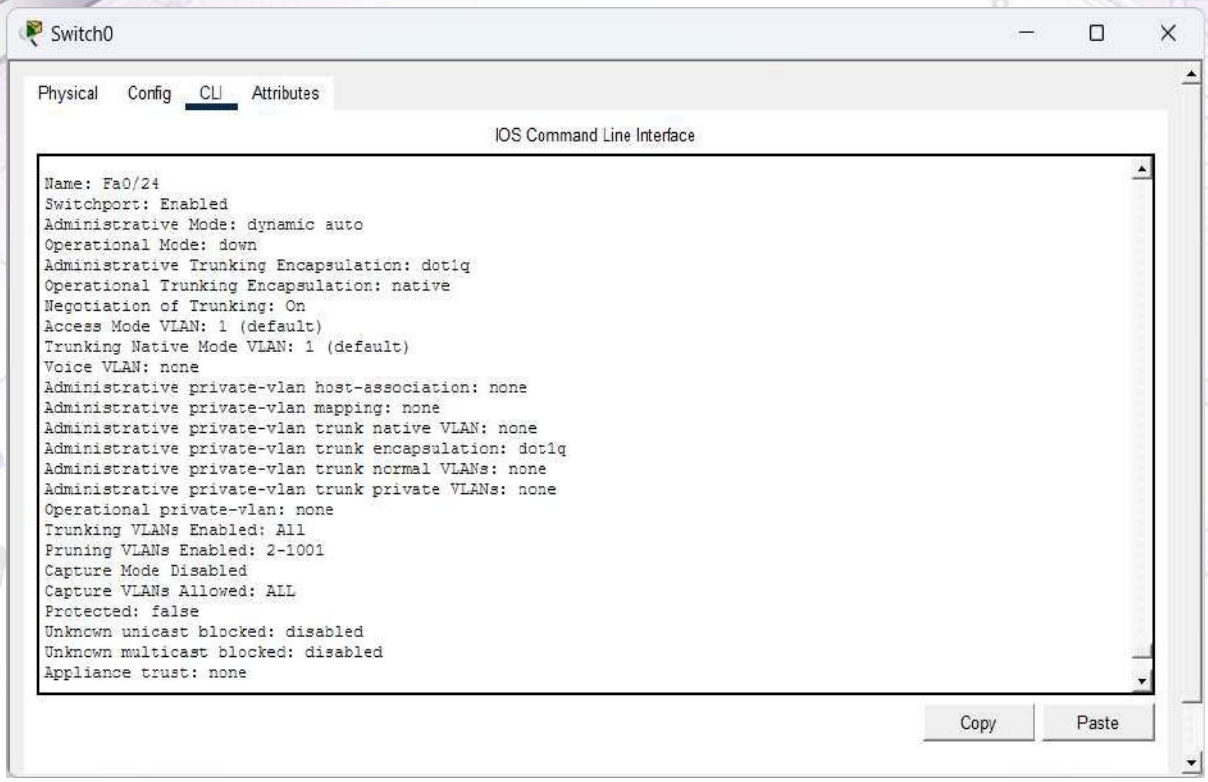
4-rasm. VLANlararo trafikning bloklangan holati.

Olingan natijalar VLAN segmentatsiyasi tarmoq xavfsizligini oshirishini va segmentlararo to‘g‘ridan-to‘g‘ri trafikni cheklashini ko‘rsatdi.

3.3. VLAN hopping xavfini modellashtirish

Tajribaning keyingi bosqichida trunk portda Dynamic Trunking Protocol (DTP) yoqilgan zaif konfiguratsiya modellashtirildi. Fa0/24 porti dynamic auto rejimida sozlandi.

ISSN 3030-3907



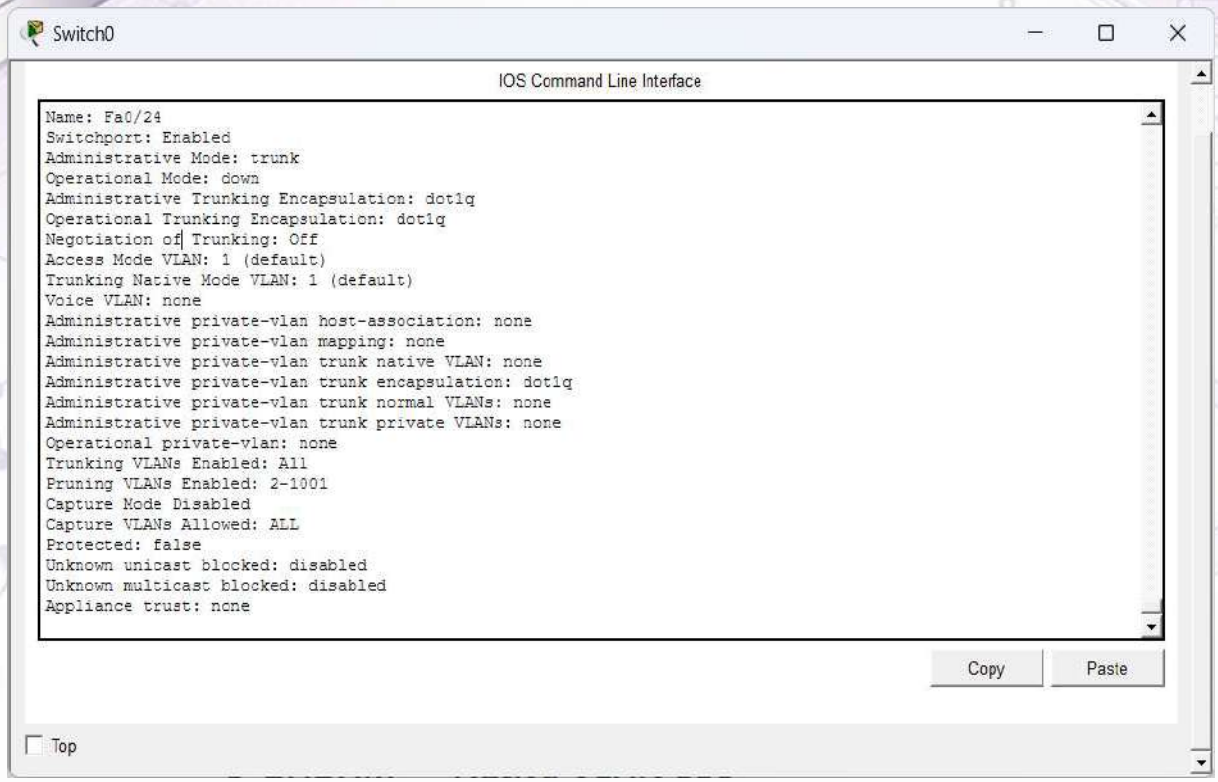
5-rasm. Dynamic auto holatidagi trunk konfiguratsiyasi.

Mazkur konfiguratsiya trunk kanalining avtomatik shakllanishiga sabab bo‘lishi mumkin. Natijada VLAN hopping hujumlari uchun xavfli muhit yuzaga keladi.

3.4. Himoya konfiguratsiyalarini qo‘llash

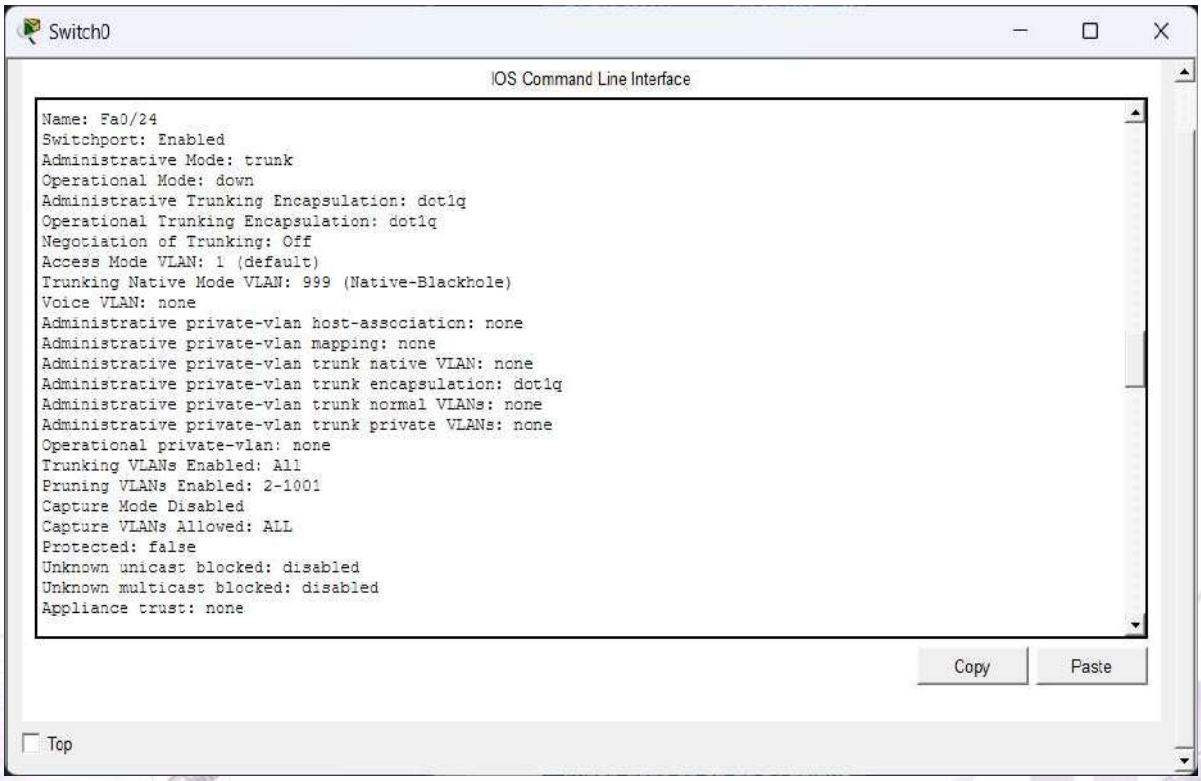
Aniqlangan xavfsizlik muammolarini bartaraf etish maqsadida trunk port statik rejimga o‘tkazildi va DTP protokoli o‘chirildi.

ISSN 3030-3907



6-rasm. Himoyalangan trunk konfiguratsiyasi.

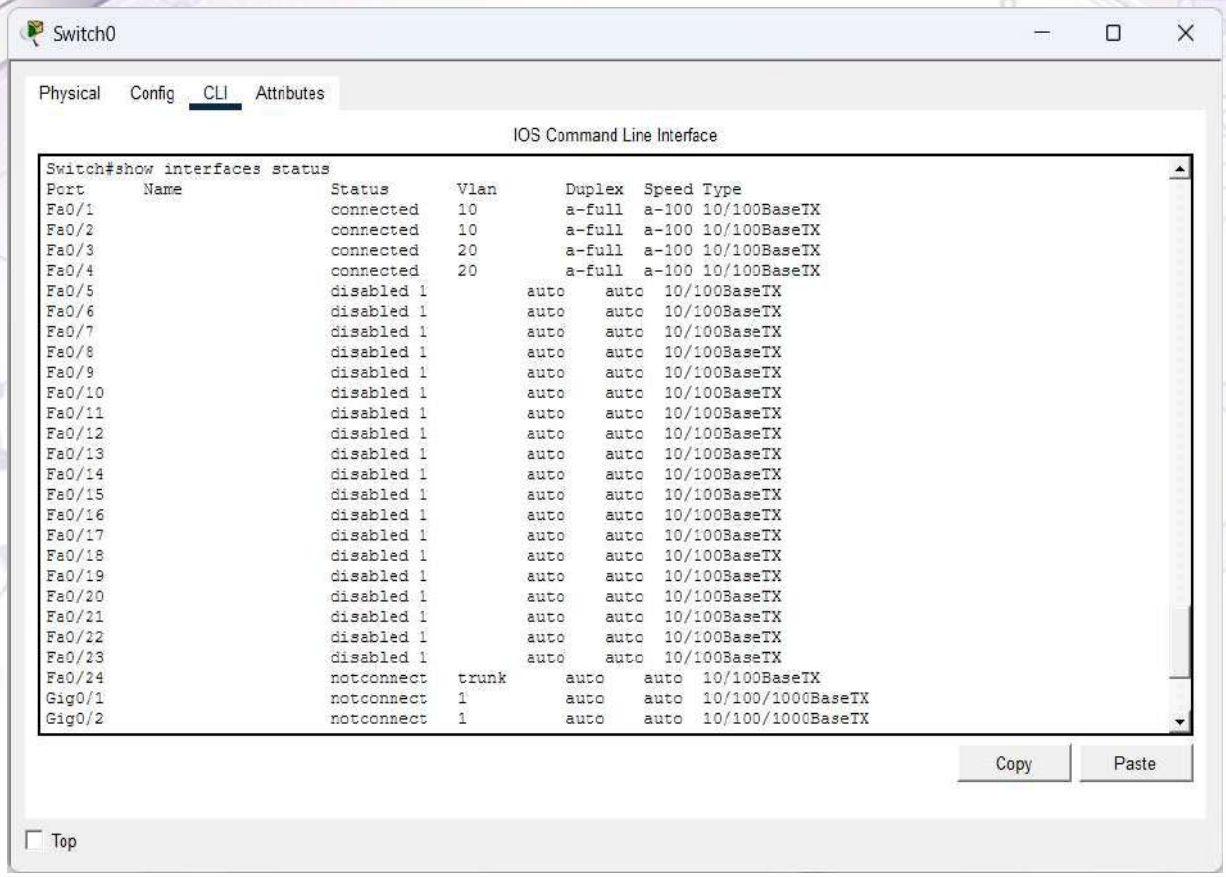
Bundan tashqari, native VLAN sifatida standart VLAN 1 o‘rniga VLAN 999 (Native-Blackhole) qo‘llanildi.



7-rasm. Native VLAN xavfsizlik konfiguratsiyasi.

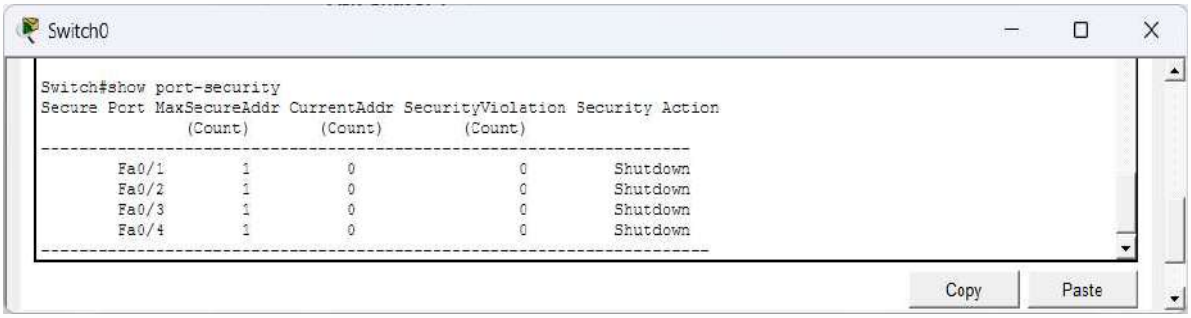
Tarmoq xavfsizligini yanada kuchaytirish maqsadida foydalanilmayotgan switch portlari shutdown holatiga o‘tkazildi.

ISSN 3030-3907



8-rasm. Keraksiz portlarning o‘chirilgan holati.

Port Security mexanizmi orqali har bir port uchun ruxsat etilgan MAC manzillar soni bittaga cheklab qo‘yildi. Noma’lum qurilma ulanganda port avtomatik bloklanadigan qilib sozlandi.



9-rasm. Port Security konfiguratsiyasi.

Yakuniy bosqichda switch qurilmasida qo‘llanilgan barcha xavfsizlik konfiguratsiyalari tekshirildi.

IV. Natijalar tahlili

Holat	Himoyadan oldin	Himoyadan keyin
VLAN hopping xavfi	Yuqori	Past
DTP zaifligi	Mavjud	Bartaraf etildi
Tarmoq segmentatsiyasi	O‘rtacha	Kuchli

ISSN 3030-3907

Ichki xavfsizlik	Cheklangan	Yuqori

O‘tkazilgan tajribalar natijasida VLAN segmentatsiyasi va qo‘shimcha xavfsizlik mexanizmlarining korxona tarmoqlarida axborot xavfsizligini sezilarli darajada oshirishi aniqlandi. DTP’ni o‘chirish, native VLAN’ni o‘zgartirish, keraksiz portlarni bloklash hamda Port Security mexanizmlaridan foydalanish ichki tarmoq tahdidlarini kamaytirishga xizmat qildi.

XULOSA.

Korxona tarmoqlarida VLAN segmentatsiyasi xavfsizlikni oshirishning samarali usullaridan biri hisoblanadi. VLAN texnologiyasi broadcast domenlarni ajratish, foydalanuvchilarni mantiqiy segmentlarga bo‘lish va ichki trafikni nazorat qilish imkonini beradi. Tadqiqot davomida trunk konfiguratsiyasidagi zaifliklar tahlil qilinib, ularni bartaraf etish usullari amaliy jihatdan ko‘rsatib berildi.

Natijalar VLAN asosidagi xavfsizlik yondashuvlari zamonaviy korxona tarmoqlarida muhim ahamiyatga ega ekanligini ko‘rsatdi. Ayniqsa, DTP protokolini o‘chirish, native VLAN’ni o‘zgartirish, foydalanilmayotgan portlarni bloklash hamda Port Security mexanizmlaridan foydalanish tarmoqning umumiy xavfsizlik darajasini sezilarli ravishda oshirdi.

FOYDALANILGAN ADABIYOTLAR

1. Cisco Networking Academy. Switching, Routing, and Wireless Essentials.
2. IEEE 802.1Q Virtual Bridged Local Area Networks Standard.
3. Odom W. CCNA 200-301 Official Cert Guide. Cisco Press.
4. Sokolov A.N. Detection of Cyber Attacks on Industrial Control Systems.
5. Dastres R. Cyber-Physical Security in Network Systems.
6. Cisco Systems. VLAN Security Best Practices.
7. IEEE Access Journal. Network Segmentation and Security Approaches.
8. Privalov A. Information Attacks Detection in Smart Networks.
9. Nassar A.A. Cyber-Attack Detection using Network Analysis.
10. Cisco Secure Network Design Guide.

ISSN 3030-3907