2019. ÁPRILIS XII. ÉVFOLYAM 4. SZÁM ÁR: 750 FT WWW.GYARTASTREND.HU

GYÁRTÁS TREND

TECHNOLÓGIAI MAGAZIN

1 Gyors beüzemelés

2 Egyszerű programozás

3 Rövid megtérülés

4 Új lehetőségek

» 26 ERŐS ÉS EGYÜTTMŰKÖDŐ

» 22 Gépikrek a kibertérben

» 48 A veszteségeket kell kiküszöbölni

PPH MEDIA a Süddeutscher Verlag Mediengruppe tagja

ISSN 1789-8935

Menedzselhető Ethernet-switchek ipari alkalmazásokhoz

HATÉKONY ÉS BIZTONSÁGOS AUTOMATIZÁLÁS

Az ipari automatizálásban használatos kommunikációs rendszerek kialakítása és követelményei jelentős mértékben eltérnek a hálózatokra általánosan vonatkozó követelményektől, a legfontosabb kritériummá a stabilitás, a megbízhatóság és az integrálhatóság vált.

Korábban a rendszer megbízhatóságának biztosítása érdekében az automatizálási rendszereket elválasztották a LAN/WAN hálózatoktól. Azonban egyre gyakrabban alkalmazzák azt a nagyvállalati LAN-hálózati struktúrát, amely mind az operatív (gyártási) technológiát (OT), mind az informatikát (IT) integrálja. A közvetlen adatcsere számos előnnyel jár, és lehetővé teszi a termelési, logisztikai és marketingfolyamatok gyorsabb optimalizálását. E területek egyre szorosabb kapcsolódása azonban új kihívásokat is magában hordoz a hálózati biztonsággal és az adatátvitellel kapcsolatban. Az alkalmazások olyan megoldásokat igényelnek, amelyek fejlett hálózati forgalomirányítást biztosítanak, redundancia- és diagnosztikai funkciókkal. A hálózati infrastruktúra kulcsfontosságú elemei a menedzselhető edge switchek. (Edge switchnek hívjuk a jellemzően két hálózat határán elhelyezkedő vagy sok állomást, azaz node-ot összefogó, azokat kiszolgáló, akár speciális feladatot, például routerelést vagy protokollkonverziót is ellátó siwtchet.) Az Antaira Technologies új LMX- és LMP-sorozatú menedzselhető edge switch sorozattal jelent meg, fejlett funkciókkal a hatékony és biztonságos hálózati menedzsment biztosítása érdekében.

» *Fejlett funkciók jellemzik a hatékony és biztonságos hálózati menedzsment biztosítása érdekében*

FEJLETT FUNKCIÓK AZ ÚJ SOROZATOKBAN

Az ipari hálózat integrációjában és a biztonsági követelményekben bekövetkezett növekedés, fejlődés egyre több és több fejlett funkció használatát követeli meg. Az ipari alkalmazásokhoz kialakított modern Antaira ipari hálózati edge switchek rendelkeznek a céges általános LAN-hálózatokban elvárt funkcionalitásokkal, de tökéletesen használhatók a robusztus, mostoha körülményeket igénylő alkalmazásokban is. A továbbiakban a modern ipari menedzselhető switch funkciók közül a legfontosabbakat mutatjuk be.

VLAN virtuális hálózatok A hálózatokat kisebb szegmensekre lehet szétválasztani, amelyek különféle feladatokra optimalizálhatók. A hálózatok szétválasztásának egyik módja a VLAN virtuális hálózatok használata, amelyek lehetővé teszik a hálózat logikai elosztását anélkül, hogy fizikai infrastruktúrája megváltozna. A VLAN használható a szórási tartomány korlátozására, ezáltal a teljes hálózat biztonságának és hatékonyságának javítására. Az egyes alhálózatokban a rendszergazdák több szoftveres eszközt, funkciót is használhatnak a hálózat működésének optimalizálására. Ha egy alhálózaton belül különböző prioritású adatok kerülnek továbbításra, ajánlott a szolgáltatásminőség (QoS, Quality Of Service) funkció használata, hogy a kritikus adatokhoz külön prioritást rendeljünk. Ha a továbbított adatok bizalmasak, vagy a hálózati hozzáférést bármilyen okból korlátozni szükséges, a menedzselhető switchben letilthatjuk a nem használt portokat, és szűrhetjük a MAC-címeket az aktív portokon.

IGMP-protokoll A protokollt a hatékony forgalomirányításra használhatjuk, amikor is nagy mennyiségű, de különböző prioritású adatok vannak a TCPIP-hálózatban. Egy, illetve kevés számú switchez csatlakoztatott eszközzel nem lehet észrevenni, ha egy standard (nem menedzselhető) switch átalakítja a multicast típusú forgalmat broadcast forgalomra. A probléma akkor lép fel, amikor egy hálózathoz csatlakoztatott eszköz a teljes broadcast forgalmat „ráereszti" a hálózatra, ami túlterhelést és jelentős késéseket eredményez. A probléma a megfelelően beállított IGMP-protokoll-paraméterek segítségével megoldható.

ERPS-protokoll Rendkívül fontos a hálózati forgalom fenntartása még több, esetlegesen párhuzamosan fellépő hiba esetén is. Ezt az eszközök és a hálózati szegmensek közötti redundáns kapcsolatok tudják biztosítani. Kivitelezéséhez egy speciális protokollt kell használni annak biztosítására, hogy ne legyenek hurkok kialakítva az Ethernet-rétegben, -hálózatban. A leggyakrabban használt az Ethernet Ring Protection Switching (ERPS) protokoll, amely nyílt szabvány, és egyaránt támogatott mindkét esetben, kereskedelmi és ipari switchek által. Az ERPS blokkolja a redundáns kapcsolatokat, és meghibásodás esetén a hálózatot kevesebb mint 50 milliszekundum alatt újrakonfigurálja.

DHCP Snooping A DHCP-protokoll fő célja, hogy automatikusan hozzárendelje az IP-címeket a hálózati eszközökhöz. A DHCP egy broadcast típusú szerviz, ebből adódóan érzékeny a különböző támadásokra. Például speciális eszközök használatával a szerver

» *Menedzselhető edge switch*

blokkolható DHCP felfedező parancsokkal. A DHCP Snooping funkció blokkolja a DHCP felfedező parancsokat, és egy megbízható porthoz rendeli hozzá a megbízható DHCP-szervert, így megakadályozza, hogy bármely más szerver csatlakozzon bármely más porthoz.

IP Source Guard Biztonsági funkció, amely a hálózati forgalom szűrésével korlátozza az IP-forgalmat a nem megbízható 2-es szintű portokon. Megakadályozza, hogy az IP-címek alapján történő megtévesztő támadásokat (a host meghamisít egy IP-címet, és egy másik hostgép IP-címét használja). Ezáltal bármely, nem a DHCP- vagy a statikus konfigurációból eredő IP-címmel rendelkező interfészen bejövő IP-forgalom szűrve lesz a nem megbízható Layer 2-portokon.

Ports Security Limit Control A megengedett MAC-címek számának korlátozásával portonként megakadályozható a jogosulatlan MAC-címmel rendelkező eszközök hozzáférése. Lehetővé teszi a biztonságos MAC-címek maximális számának bekonfigurálását a VLAN-hálózatok trunkportjain.

ACL (Access Control Lists) Lehetővé teszi a hálózati forgalmi szabályok létrehozását. Az ACL-listák létrehozásával egy bejövő forgalom elfogadható vagy elutasítható, ezáltal szabályozva a hálózathoz vagy bizonyos erőforrásokhoz való hozzáférést. Minden ACL-lista tartalmaz egy, a bejövő forgalomra vonatkozó szabályok csoportját.

Authentication (hitelesítés) 16 engedélyezési és hitelesítési szintet használnak a Radius- vagy a Tacacs+- (Cisco) protokollok. A kezelő IP- és MAC-címének ellenőrzése lehetővé teszi a felhasználó ellenőrzését. Az inaktív felhasználók automatikus kijelentkeztetése megakadályozza az illetéktelen hozzáférést.

■ **Michal Sadowski, Orosi Levente**

info@axtek.hu
www.axtek.hu