

**A NetFlow bemutatása**

A NetFlow egy Cisco IOS technológia, amely statisztikákat szolgáltat a Cisco forgalomirányítókon, illetve többrétegű kapcsolókon áthaladó csomagokról. A NetFlow egy szabvány az IP működési adatok IP-hálózatokon történő gyűjtésére.

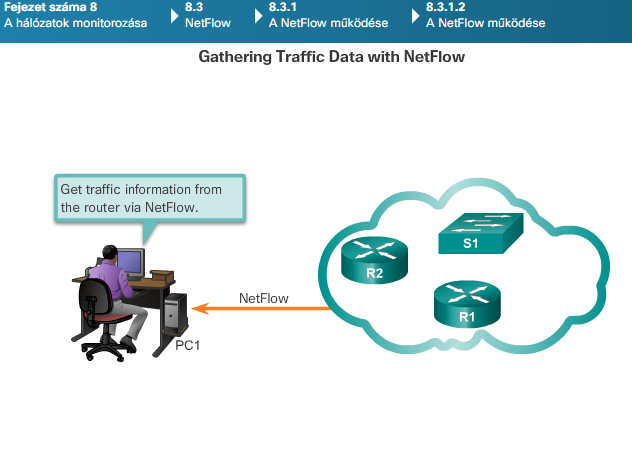
Történelmileg a NetFlow technológiát azért fejlesztették ki, mert a hálózati szakembereknek szüksége volt egy egyszerű és hatékony módszerre a TCP/IP forgalom nyomon követésére a hálózaton, és az SNMP nem volt elégséges e célokra. Míg az SNMP megkísérli, hogy nagyon széles körű hálózati menedzsment funkciókat és lehetőségeket nyújtson, a NetFlow arra fókuszál, hogy statisztikákat gyűjtsön a hálózati eszközökön átfolyó IP-csomagokról.

A NetFlow adatokat szolgáltat a hálózati és biztonsági ellenőrzéshez, hálózattervezéshez, forgalmi elemzéshez a hálózat szűk keresztmetszeteinek azonosítására, valamint IP forgalomszámlázási célokra. Az ábrán például a PC1 a PC2-höz kapcsolódik HTTPS vagy ahhoz hasonló alkalmazás segítségével. A NetFlow nyomon tudja követni az alkalmazás kapcsolatait, a csomagok és bájtok számát az adott alkalmazás adatáramlásán belül. Ezután átadja a statisztikákat egy külső szervernek, az úgynevezett NetFlow gyűjtőnek (collector).

A NetFlow ellenőrzési szabvánnyá vált, és ma már széles körben támogatott a hálózati iparágon belül.

A rugalmas NetFlow (Flexible NetFlow) a legújabb NetFlow technológia. A Flexible NetFlow javítja az "eredeti" NetFlow-t azon képesség hozzáadásával, hogy a forgalomelemzési paraméterek testre szabhatók a hálózati rendszergazda konkrét igényeinek megfelelően. A Flexible NetFlow megkönnyíti az összetettebb rendszerek forgalmi elemzési és adatexportálási beállításainak létrehozását, az újra felhasználható konfigurációs elemek révén.

A Flexible NetFlow a 9-es verzió export formátumát használja. A NetFlow 9-es verziójú export formátumának megkülönböztető jellemzője, hogy sablon-alapú. A sablonok az adatrögzítési formátum egy bővíthető modelljét jelentik. Ez a szolgáltatás teszi lehetővé a jövőbeni fejlesztéseket a Netflow szolgáltatások terén anélkül, hogy egyidejűleg megkövetelné az alapvető adatáramlás-rögzítési formátum módosításait. Fontos megjegyezni, hogy sok hasznos Flexible NetFlow parancsot vezettek be a Cisco IOS 15.1-ben.



# A NetFlow működése

Sok lehetséges felhasználási módja van azoknak a NetFlow által biztosított statisztikáknak; a legtöbb szervezet azonban az alábbi néhány (vagy az összes) fontos adat begyűjtése céljából használja:

* Annak mérése, hogy ki melyik hálózati erőforrást használja, és milyen célból.
* Számlázás és erőforrás-átcsoportosítás a kihasználtságnak megfelelően.
* A mért adatok felhasználása a hatékonyabb hálózattervezés érdekében, hogy az erőforrások elosztása és telepítése jól igazodjon a felhasználói elvárásokhoz.
* A kapott információ segítségével jobban alakíthassuk és testre szabhassuk az elérhető alkalmazások és szolgáltatások körét, hogy megfeleljen a felhasználók igényeinek és az ügyfélszolgálati követelményeknek.

Ha összehasonlítjuk az SNMP és a NetFlow funkcionalitását, az SNMP-t úgy képzelhetjük el, mint egy távirányító szoftvert egy pilóta nélküli járműhöz; a NetFlow-t pedig mint egy egyszerű, de annál részletesebb telefonszámlát. A telefonos híváslisták hívásonkénti és összesített statisztikákat biztosítanak, amelyek lehetővé teszik az előfizető számára, hogy nyomon követhesse a hosszú vagy gyakori hívásokat, esetleg azokat, amelyeket nem kellett volna kezdeményezni.

Az SNMP-vel ellentétben a NetFlow a küldésen alapuló ("push-based") modellt használja. A gyűjtő egyszerűen figyeli a NetFlow forgalmat, és a hálózati eszközök a felelősek az adatok elküldéséért, a gyorsítótárukban bekövetkezett változások alapján. Egy másik különbség a NetFlow és az SNMP között, hogy a NetFlow csak a forgalmi statisztikákat gyűjti, amint az ábrán látható, míg az SNMP begyűjthet számos más minőségi mutatót is, mint például: interfészhibák, CPU-használat és memóriahasználat. Másrészt, a NetFlow által gyűjtött forgalmi statisztikák sokkal nagyobb részletességűek, mint azok, amiket az SNMP-vel lehet összegyűjteni.

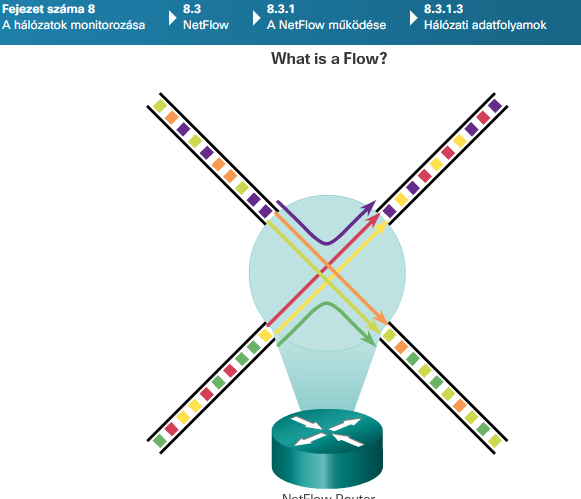
**MEGJEGYZÉS:**: Ne keverjük össze a NetFlow célját és az eredményeit egy csomagelfogó (packet capture) hardverével vagy szoftverével. Amíg a csomagelfogók rögzítenek minden lehetséges információt, ami kilép vagy belép a hálózati eszközbe későbbi elemzés céljából, a NetFlow a konkrét statisztikai adatokat célozza meg.

Amikor a Cisco létrehozta a NetFlow-t, két kritérium nyújtott útmutatást annak elkészítéséhez:

* A NetFlow-nak teljesen átláthatónak kell lennie a hálózati alkalmazások és eszközök számára.
* A NetFlow-t nem kell minden eszköznek támogatnia és futtatnia a hálózaton, hogy működjön.

Ezeknek a tervezési feltételeknek a biztosításával a NetFlow nagyon könnyen megvalósítható a legösszetettebb modern hálózatokban is.

**MEGJEGYZÉS:**: Bár a NetFlow egyszerűen megvalósítható és átlátható a hálózat számára, további memóriát fogyaszt a Cisco eszközökön, mivel tárolja a rögzített információt a készülék gyorsítótárában. A gyorsítótár alapértelmezett mérete a platformtól függ, és a rendszergazda testre szabhatja ezt az értéket.



**Hálózati adatfolyamok**

A NetFlow statisztikai nyilvántartásokra bontja le a TCP/IP kommunikációt az adatfolyam fogalmát felhasználva. Az adatfolyam (flow) a csomagok egyirányú áramlása egy adott forrásrendszer és egy adott célállomás között. Az adatfolyam fogalma az ábrán látható.

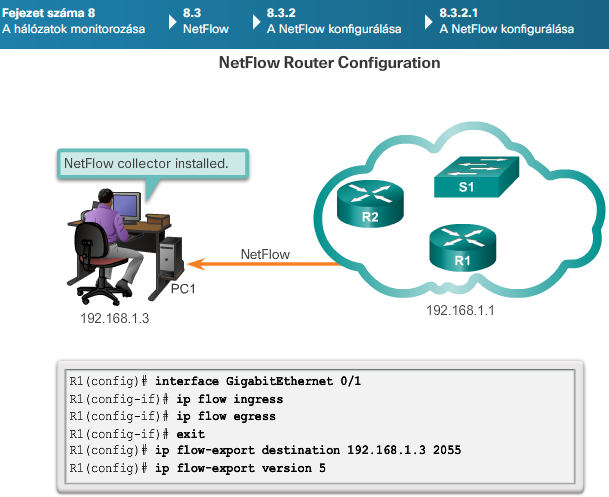
A TCP/IP köré épülő NetFlow számára a forrást és a célt meghatározzák a hálózati rétegbeli IP-címek és a szállítási rétegbeli forrás- és cél-portszámok.

A NetFlow technológia több generációt ért meg, amelyek egyre kifinomultabban írták le a forgalmat, de az "eredeti NetFlow" hét mező kombinációja segítségével határozta meg az adatfolyamokat. Amennyiben e mezők valamelyikében eltérő értéket mutat egy másik csomag, arról biztonságosan ki lehet jelenteni, hogy különböző adatfolyamhoz tartozik:

* forrás IP-cím
* cél IP-cím
* forrás portszám
* cél portszám
* 3. rétegbeli protokoll típusa
* Type of Service (TOS) jelölés
* bejövő logikai interfész

Az első négy mező, amit a NetFlow az adatfolyam azonosítására használ fel, ismerős kell, hogy legyen. A forrás és cél IP-címek, valamint a forrás- és a célportok azonosítják a kapcsolatot a forrás- és célalkalmazás között. A 3. rétegbeli protokoll típusa azonosítja azt az adott típusú fejlécet, amely az IP-fejlécet követi (általában TCP vagy UDP, de más lehetőség is van, pl.: ICMP). A ToS bájt az IPv4 fejlécben információt ad arról, hogy az eszközöknek miként kell alkalmazni a szolgáltatásminőségi (QoS) szabályokat a csomagokra az adott adatfolyamon belül.

A Flexible NetFlow még több lehetőséget támogat a forgalmi adatok rögzítéséhez. A Flexible NetFlow lehetővé teszi, hogy a rendszergazda határozza meg a rögzítendő adatokat az adatfolyamot figyelő gyorsítótár számára. Ez a felhasználó által definiált választható és kötelező mezők megadásával érhető el, hogy testre szabva az adatgyűjtést, az megfeleljen az adott követelményeknek. Amikor meghatározzuk az adatokat a Flexible NetFlow gyorsítótár számára, ezeket felhasználó által meghatározott rekordoknak nevezzük. Az adatfolyamokhoz adott opcionális mezőkben lévő értékek további információt adnak az adatforgalom áramlásáról. Egy opcionális mező értékében bekövetkező változás nem hoz létre új adatfolyamot.



**A NetFlow konfigurálása**

A NetFlow megvalósítása egy forgalomirányítón:

**1. lépés: A NetFlow adatrögzítés beállítása** - a NetFlow rögzíti az adatokat a bejövő (ingress) és kimenő (egress) csomagokból.

**2. lépés: A NetFlow adatexport beállítása** - A NetFlow gyűjtőeszköz IP-címét vagy nevét meg kell adni, valamint azt az UDP portot, amelyiken a NetFlow gyűjtő figyel.

**3. lépés: A NetFlow működésének és statisztikáinak ellenőrzése** - A NetFlow beállítását követően az exportált adatok elemezhetők egy munkaállomáson, amin fut egy olyan alkalmazás, mint például a SolarWinds NetFlow Traffic Analyzer, a Plixer Scrutinizer vagy a Cisco NetFlow Collector (NFC). Minimálisan támaszkodni lehet többféle **show** parancs kimenetére is, magán a forgalomirányítón.

Néhány szempont a NetFlow konfigurációjához:

* Az újabb Cisco forgalomirányítók, mint például az ISR G2 sorozat, támogatja mind a NetFlow-t, mind a Flexible NetFlow-t.
* Az újabb Cisco kapcsolók, mint például a 3560-X sorozatúak, támogatják a Flexible NetFlow-t; azonban néhány kapcsoló, mint például a Cisco 2960 sorozatúak, nem támogatják ezeket.
* A NetFlow több memóriát fogyaszt. Ha a Cisco hálózati eszköz memóriamennyisége korlátozott, a NetFlow gyorsítótár méretét előre be lehet állítani, hogy kevesebb bejegyzést tartalmazzon. Az alapértelmezett gyorsítótár mérete függ a platformtól.
* A NetFlow gyűjtő szoftver követelményei változóak. Például a Scrutinizer NetFlow szoftver egy Windows munkaállomáson 4 GB RAM-ot és 50 GB lemezterületet igényel.

**MEGJEGYZÉS:**: A hangsúly itt az eredeti NetFlow (a Cisco dokumentáció alapján a továbbiakban egyszerűen NetFlow) Cisco forgalomirányítókon történő beállításán van. A Flexible Netflow konfigurációja túlmutat a tanfolyam keretein.

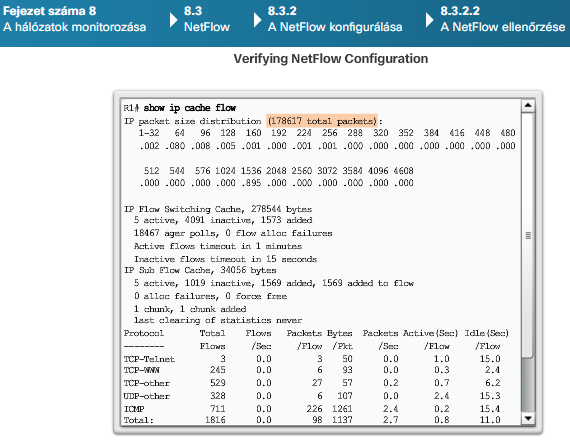
A NetFlow adatfolyam egyirányú. Ez azt jelenti, hogy egy felhasználói kapcsolathoz egy alkalmazás esetén két NetFlow adatfolyam létezik, mindkét irányban egy-egy. A rögzítendő adatok meghatározása interfész-konfigurációs módban:

* A NetFlow adatok nyomon követése az interfészen bejövő csomagok esetében az **ip flow ingress** paranccsal történik.
* A NetFlow adatok nyomon követése az interfészen kimenő csomagok esetében az **ip flow egress** paranccsal történik.

Ahhoz, hogy engedélyezzük az adatok küldését a NetFlow gyűjtőhöz, több dolgot kell beállítani globális konfigurációs módban:

* **a NetFlow gyűjtő IP-címét és UDP portszámát -** Használjuk az **ip flow-export destination** *ip-cím udp-port* parancsot. A gyűjtő egy vagy több porttal rendelkezik alapértelmezés szerint az adatrögzítéshez. A szoftver lehetővé teszi a rendszergazda számára, hogy megadja, mely porton vagy portokon fogadja el a NetFlow adatokat. Néhány gyakori UDP-port erre a célra a 99, 2055 és 9996.
* **(Opcionális) A NetFlow gyűjtőnek elküldött bejegyzések formázására használt verzióját -** Használjuk az **ip flow-export version** *verzió* parancsot. A NetFlow az adatokat UDP segítségével exportálhatja, öt formátum egyikében (1, 5, 7, 8 és 9). A 9-es verzió a legsokoldalúbb export adatformátum, de nem kompatibilis visszafelé a korábbi verziókkal. Az 1-es változat az alapértelmezett, ha nem adjuk meg az 5-ös verziót. Az 1-es verziót csak akkor használjuk, ha ez az egyetlen NetFlow adatexport formátum változat, amit támogat a NetFlow gyűjtő szoftver.
* **(Opcionális) A a csomagok forrásaként feltüntetett forrásinterfészt a küldésnél** - Használjuk az **ip flow-export source** *típusszám* parancsot.

Az ábra egy egyszerű NetFlow konfigurációt mutat be. Az R1 forgalomirányító G0/1 interfészének IP-címe 192.168.1.1. A NetFlow gyűjtő IP-címe 192.168.1.3, és úgy állították be, hogy rögzítse az adatokat a 2055-ös UDP-porton. A G0/1 interfészen a ki- és bemenő forgalmat egyaránt figyeljük. A NetFlow adatok továbbítása az 5-ös verziójú formátumban történik.



**A NetFlow ellenőrzése**

Miután ellenőriztük, hogy a NetFlow megfelelően működik, megkezdődhet az adatgyűjtés a NetFlow gyűjtőn. A NetFlow ellenőrzését a gyűjtőn tárolt adatok vizsgálatával végezzük el. Az a minimum, hogy ellenőrizzük a helyi NetFlow gyorsítótárat a forgalomirányítón, hogy gyűjti-e az eszköz az adatokat.

A NetFlow-t az alábbiak szerint állították be az R1 forgalomirányítón:

* a G0/1 interfész IP-címe 192.168.1.1/24
* a ki- és bejövő forgalmat is figyeli a NetFlow
* a NetFlow gyűjtő a 192.168.1.3/24 címen van
* a NetFlow UDP gyűjtőport a 2055
* a NetFlow 5-ös verziójú export formátumot használ

Az összefoglaló naplózási statisztikák megjelenítéséhez, valamint annak kiíratásához, hogy mely protokoll teszi ki a forgalom legnagyobb részét, és hogy melyik állomások között halad a forgalom, használjuk a **show ip cache flow** parancsot felhasználói vagy privilegizált EXEC módban. A parancsot az R1-en adtuk ki, hogy ellenőrizzük a NetFlow konfigurációt, ahogy az 1. ábrán is látható. A parancs kimenete részletezi, hogy melyik protokoll teszi ki a forgalom legnagyobb részéét, és mely állomások között zajlik a forgalom. Az 1. ábra táblázata leírja a jelentősebb mezőket, amik az adatfolyam-gyorsítótár megjelenített soraiban láthatók.

A kimenet az elején megerősíti, hogy a forgalomirányító adatokat gyűjt. Az első kiemelt bejegyzés 178617 csomagot sorol fel, amit a NetFlow megfigyelt. A kimenet a végén három adatáramlásról jelez statisztikát, a kiemelt egy aktív HTTPS-kapcsolatnak felel meg a NetFlow gyűjtő és az R1 között. Ezen kívül hexadecimálisan mutatja a forrásportot (SrcP) és célportot is (DstP).

**MEGJEGYZÉS:**a hexadecimális 01BB egyenlő a decimális 443-mal, a jól ismert HTTPS TCP-porttal.

A 2. ábra bemutatja a jelentősebb mezőket a gyorsítótárból a **show ip cache flow** parancs kimenetében.

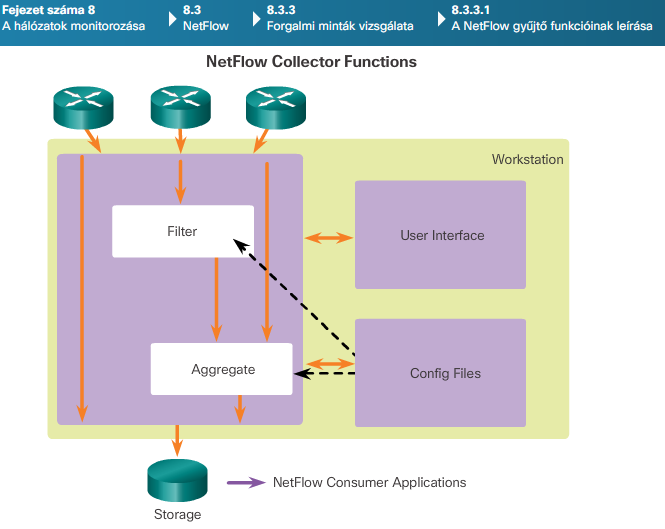
A 3. ábra bemutatja a jelentősebb mezőket a protokoll szerinti tevékenységekből a **show ip cache flow** parancs kimenetében.

A 4. ábra mutatja a jelentősebb mezőket a NetFlow által rögzített sorokból a **show ip cache flow** parancs kimenetében.

Bár a **show ip cache flow** parancs kimenete megerősíti, hogy a forgalomirányító adatokat gyűjt, annak ellenőrzésére, hogy a NetFlow a megfelelő interfészeken és a megfelelő irányban van beállítva, használjuk a **show ip flow interface** parancsot, az 5. ábrán látható módon.

Az exportálási paraméterek konfigurációjának ellenőrzéséhez használjuk a **show ip flow export** parancsot, az 5. ábrán látható módon. Az első kiemelt sor azt mutatja, hogy be van kapcsolva a NetFlow 5-ös verziójú export formátuma. Az utolsó kiemelt sorok az 5. ábrán azt mutatják, hogy 1764 adatfolyamot exportáltunk 532 darab UDP-adatcsomag formájában a NetFlow gyűjtőnek a 192.168.1.3 címre, a 2055-ös porton.

Használjuk a parancsszimulátort a 6. ábrán a NetFlow R1 forgalomirányítón való konfigurálásához és ellenőrzéséhez.



**A NetFlow gyűjtő funkcióinak leírása**

A NetFlow gyűjtő egy szoftveralkalmazást futtató állomás. Ez a szoftver nyers NetFlow adatok kezelésére specializálódott. A gyűjtő beállítható úgy, hogy információkat kapjon számos hálózati eszköztől. A NetFlow gyűjtők az adatokat begyűjtik és elrendezik a hálózati rendszergazda által előírt módon, a szoftver korlátain belül.

Egy gyűjtőn a NetFlow adatok meghatározott időközönként kiírásra kerülnek a meghajtóra. A rendszergazda több begyűjtési rendszert vagy szálat futtathat egyidejűleg. Például különböző adatdarabok tárolhatók a tervezés, külön a számlázás támogatására; a NetFlow gyűjtő könnyen előállítja a megfelelő összegzési sémákat.

Az 1. ábra egy NetFlow gyűjtőt mutat, ami passzívan figyeli az exportált adatcsomagokat. A NetFlow gyűjtő alkalmazás egy nagy teljesítményű, könnyen használható, skálázható megoldás a több eszköztől származó export adatok befogadására és feldolgozására. A szervezet szándéka a felhasználásra vonatkozóan változó, de gyakran az a cél, hogy támogassuk a kritikus adatáramlásokat, amik a fogyasztói alkalmazásokhoz kapcsolódnak. Ezek közé tartozik a könyvelés, számlázás, valamint a hálózat tervezése és ellenőrzése.

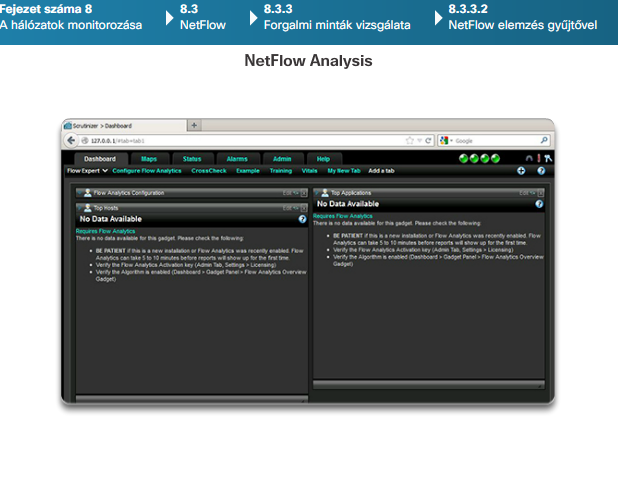
Számos NetFlow gyűjtő van a piacon. Ezek az eszközök lehetővé teszik a forgalom elemzését a hálózaton úgy, hogy megmutatják a leginkább aktív állomásokat, a leggyakrabban használt alkalmazásokat, és egyéb eszközöket adnak a forgalmi adatok mérésére, a 2. ábrán látható módon. A NetFlow gyűjtő megjeleníti a különböző fajta forgalmakat (web, e-mail, FTP, peer-to-peer, stb.) a hálózaton, valamint a forgalom nagy részét küldő és fogadó eszközöket. Az adatgyűjtés megmutatja a hálózati rendszergazdának a legtöbbet forgalmazó állomásokat és a legaktívabb figyelőket is. Mivel az adatok hosszabb időre megmaradnak, az utólagos forgalomelemzéssel meghatározhatók a hálózathasználati tendenciák.

A NetFlow elemzők használata alapján a hálózati rendszergazda azonosítani tudja a következőket:

* Kik a legaktívabb forgalmazók és kivel kommunikálnak?
* Milyen weboldalakat látogatnak rutinszerűen, és mit töltenek le?
* Ki generálja a legnagyobb forgalmat?
* Van-e elegendő sávszélesség a kritikus tevékenységek biztosítására?
* Ki foglalja le a sávszélességet?

A NetFlow gyűjtő által elemezhető információ mennyisége a használt NetFlow változattól függően eltérő lehet, mivel a különböző export formátumok különböző rekordtípusokból állnak. A NetFlow rekord tartalmazza a részletes információkat az adatfolyamot alkotó aktuális forgalomról.

A NetFlow gyűjtő valós idejű megjelenítést és elemzést biztosít a rögzített és összesített forgalmi adatokról. A forgalomirányítók és a támogatott kapcsolók is megadhatók, valamint az összesítési séma és az időintervallumok az adatok tárolására, még a következő időszakos vizsgálatot megelőzően. Sorba rendezhetjük és megjeleníthetjük az adatokat olyan módon, amely érthető a felhasználók számára: oszlopdiagramokba, tortadiagramokba vagy hisztogramokba rendezve a jelentéseket. Az adatokat ezután exportálni lehet táblázatokba (pl.: a Microsoft Excelbe), részletes elemzés, trendek és jelentések készítése céljából.



**NetFlow elemzés gyűjtővel**

A Plixer International kifejlesztette a Scrutinizer nevű NetFlow analizátor szoftvert. A Scrutinizer egy a sok lehetőség közül, hogy rögzítsük és elemezzük az adatokat egy NetFlow gyűjtőn.

Emlékezzünk a konfigurációra az előző témából:

* a G0/1 interfész IP-címe 192.168.1.1/24
* a ki- és bejövő forgalmat is figyeli a NetFlow
* a NetFlow gyűjtő a 192.168.1.3/24 címen van
* a NetFlow UDP gyűjtőport a 2055-ös
* a NetFlow 5-ös verziójú export formátumot használ

A Scrutinizer szoftvert a 192.168.1.3/24 című NetFlow gyűjtőre telepítették.

Az 1. ábra mutatja a szoftver felületét a Scrutinizer alkalmazás megnyitásakor.

A 2. ábra annak eredményét jeleníti meg, ha a Status lapra kattintunk az alkalmazás futása közben. A szoftver a következő üzenetet jeleníti meg: "Adatfolyamokat észlelek, kérjük várjon, amíg a Scrutinizer előkészíti az első jelentéseket".

A 3. ábra a Status képernyő állapotát mutatja néhány perc múlva. Az R1 forgalomirányítón a cisco.com tartománynév lett beállítva.

Az SNMP-konfiguráció az előző részből még mindig aktív az R1-en. A Scrutinizer szoftvert konfiguráltuk a *batonaug* közösségi karakterlánc értékre az **Admin Settings** fülön. Amikor az SNMP-kapcsolatra kattintunk az R1.cisco.com alatt a bal oldali panelen, a kijelzőn a 4. ábra jelenik meg. Ez mutatja az alapvető forgalomelemzést az R1 és a NetFlow gyűjtő között az SNMPv2c segítségével. A Multi Router Traffic Grapher (MRTG) szabad szoftver, amit sok hálózati rendszergazda használ alapvető forgalomelemzésre. A Scrutinizer alkalmazás magába foglalja az MRTG-t, így a 4. ábra grafikonjait is az MRTG készítette. A felső grafikon mutatja a bejövő, az alsó grafikon pedig a kimenő forgalmat az R1 forgalomirányító G0/1 interfészén.

Végül az 5. ábrán a **Dashboard** fül jeleníti meg a tényleges NetFlow adatokat a Top Hosts (legaktívabb állomások) és Top Applications (legtöbbet használt alkalmazások) tekintetében. A Scrutinizer szoftverben több tucat ilyen eszköz érhető el az adatok különböző katagóriák szerinti megjelenítésére. Az 5. ábrán a legaktívabb eszköz az R1, a legnagyobb mennyiségű forgalommal az R1 és a NetFlow gyűjtő között. A legfontosabb alkalmazás a HTTPS, majd az SNMP, a HTTP, az SSH, az ICMP és a NetBIOS következik.