INTERNETOVÉ TECHNOLOGIE – SERVER SIDE P6
2009-03-24

PLOŠNÉ, SOUVISLÉ SLEDOVÁNÍ ROZSÁHLÝCH (IP) SÍTÍ:
…jako podpora při řešení provozních anomálií a bezpečnostních incidentů

Tomáš Košňar
Cesnet, z. s. p. o.
kosnar@cesnet.cz

Důležité principy IP sítí a síťové hierarchie:
- ✓ Přepínání paketů, princip přenosu dat
- ✓ Hierarchická adresace, směrování, schémata doručování
- ✓ Princip vrstev & datová enkapsulace

Přepínání paketů:
- ✓ Přenášené datové bloky (pakety – diagramy) nesou informaci nutnou k přenosu na cílové místo.
- ✓ Uzel připojení k síti může v principu komunikovat s jakýmkoli jiným připojeným uzlem – zajišťuje funkce sítě (zpravidla existuje více možných cest pro přenos mezi dvěma uzly).
- ✓ V případě **IP sítí:**
  - Paket tj. datový blok – datagram
  - IPv4 – 20 B – 64 KiB
  - IPv6 – 40 B – 64 KiB, za určitých okolností (dáno MTU) i „jumbograms“ až do 4 GiB

Hierarchická adresace:
- ✓ Identifikace – základ komunikace
- ✓ IPv4 – 4 Byte, 2^{32} kombinací
- ✓ IPv6 – 16 Byte, 2^{128} kombinací
- ✓ **Hierarchický integrátor:**
  - Umožňuje „strukturovat“ síť
  - „Síťová část“ + „uzlová část“ – rozhoduje maska

Směrování:
- ✓ Způsob přenosu dat – směrování (routing)
- ✓ V rámci stejní IP sítě přímo
- ✓ Do jiné IP sítě prostřednictvím směrovače (router)

Schéma doručování:
- ✓ V závislosti na adrese
- ✓ Vyhrazené části adresového prostoru
- ✓ Anycast
- ✓ Broadcast
- ✓ Multicast
- ✓ Unicast

Princip vrstev:
- ✓ IP protokol sám o sobě nestačí
- ✓ Síťová hierarchická struktura – princip vrstev (modely TCP/IP, OSI)
- ✓ Aplikační vrstva – http, SMTP
- ✓ Transportní vrstva – TCP, UDP
- ✓ Sítová vrstva – IP
- ✓ Linková vrstva – např. Ethernet
- ✓ **Princip enkapsulace** (zapouzdření):
  - Hierarchie vrstev promítnutá do struktury přenášeného datového bloku – příklad Ethernet paketu, tj. rámce.
  - HTTP protokol => TCP segment => IP datagram => Ethernet rámec (frame)

Nižší vrstvy – média a způsob využití:
- ✓ Přenos pod „paketovými vrstvami“
- ✓ Volný prostor, metalické vodiče, optická vlákna
- ✓ Optické vlákno – nosné technologie
- ✓ Vícenásobné využití optického vlákna
- ✓ WDM – frekvenční multiplex

Komplexní strukturované sítě:
- ✓ Vše dohromady s možnostmi vyšších vrstev
- ✓ Vícenásobné využití média => kanály – virtuální média („pseudodrát“)
- ✓ Strukturování sítě na úrovni přenášených datových bloků (VLAN) – přiřazení paketů do skupin => rozšíření paketů
- ✓ Rekurze – síť v síti, emulace nižší vrstvy pomocí vlastností vyšší vrstvy

Závěry a prognózy ve vztahu k plošnému sledování sítí:
- ✓ Komplexní, relativně složité, multitechnologické prostředí
- ✓ Roste hybridní charakter – poskytovány služby více vrstev
- ✓ Roste míra vizualizace

Proč sledovat síť?
- ✓ Co nelze měřit a sledovat, to nelze dobře ani efektivně řídit
- ✓ Zajistit bezchybné a optimální fungování
- ✓ Zabránit zneužití

Proč sledovat souvisle a plošně?
- ✓ **Efektivní identifikace:**
  - Silných a slabých míst
  - Proporce využití zdrojů
  - Trendy v chování uživatelů
- ✓ **Výrazně zvyšuje efektivitu řešení:**
  - Provozních problémů, anomálií
  - Bezpečnostních incidentů

Vhodná nástroje pro plošné a souvislé sledování sítí:
- ✓ Neexistuje nic univerzálního – mnoho vrstev, mnoho technologií, mnoho výrobců
- ✓ Přijaté řešení – rozdělení problematiky do 2 oblastí:
  - Sledování infrastruktury sítě
  - Sledování IP provozu sítě

Plošné sledování infrastruktury sítě:
- ✓ SNMP – Simple Network Management Protocol
- ✓ Informace získané z aktivních prvků sítě – SNMP v obecné podobě i pro management a zasílání varovných zpráv
- ✓ Vhodné pro plošné, v čase souvislé sledování
- ✓ Nevhodné pro sledování dějů v reálném čase (s výjimkou „snmp-trap“)
- ✓ Databáze MIB – Media Information Base
- ✓ Definice MIB objektů – pomocí ASN.1 dle „Structure of Management Information Version 2 SMIv2)
- ✓ SNMP – po zpracování získaných hodnot lze vytvořit náhled jako na infrastrukturu sítě
- ✓ Principiálně dostupné informace
- ✓ Zpravidla souhrnné (anonymizované informace)
- ✓ Principiálně Nedostupné informace

Plošné sledování IP provozu sítě:
- ✓ Provozem míněna v tomto kontextu data přenášená prostřednictvím rodiny IP protokolů
- ✓ Informace o provozu na bázi toků (Flow)

- Vytvářený z údajů získaných přenášených datových bloků (datagramů)
- Koncept NetFlow

✓ Informace o provozu na bázi Flow – vztah k ochraně soukromí uživatelů
- Pouze technologické identifikátory
- Žádná vazba na osobní identifikátory

✓ Struktura záznamu:
- Identifikátory toku:
  - Základní veličiny identifikující tok
  - Všechny pakety příslušné danému toku mají tyto údaje stejné
  - Tyto údaje tvoří identifikátor toku
- Objemové ukazatele a časové informace – agregované údaje, jsou modifikovány s každým dalším paketem příslušným danému toku
- Atributy toku

✓ Vzorkování – metoda snížení absolutního množství dat ke zpracování (trade off – ztráta vypovídací úrovně)

✓ Schéma sledování provozu:
- O provozu, který „neteče přes zdroj“ Flow záznamů se tím to způsobem nic nedozvíme
- O provozu, který „teče přes více zdrojů“ Flow záznamů získáme vícenásobné informace

✓ Systém FTAS – podpora při řešení bezpečnostních incidentů