Úvod do pokročilých síťových technologií

Petr Grygárek

Systémové síťové služby

Syslog

- Agregace systémových zpráv z různých prvků na společném serveru
  - snadnější možnost vyhledávání vztahů mezi událostmi
- Syslog server – mnoho implementací (syslogd)
- Syslog servery lze řetězit
  - filtrování a přeposílání zpráv
- Klientská komponenta definována pomocí Facility
- Několik úrovní urgence – Severity
- Protokol (nad UDP nebo TCP) standardizován IETF (RFC 3164)
  - klientské knihovny pro většinu jazyků
- Zprávy zasílány jako cleartext
  - možnost obalení SSL wrapperem
- Možnost inteligentního dělení zpráv do více souborů na Syslog serveru

Network Time Protocol (NTP)

- synchronizace vnitřních hodin počítačů po paketové síti s proměnným zpožděním od časových serverů
  - používá tzv. Marzullův algoritmus, dosažitelná přesnost v řádu ms
- NTP servery různých úrovní (stratum)
  - servery stratum 1 odvozují čas z externích hodin (GPS, rádiový signál)
- NTP klienti
  - k dispozici formou NTP démona nebo knihoven
- Simple NTP (SNTP)
  - pro embedded systémy
  - menší přesnost - nekalkuluje s proměnným zpožděním v síti
- Využití:
  - bezpečnostní technologie (certifikáty, anti-replay mechanismy, ...)
  - Logování se skutečným časem
  - Time-based ACL
  - ...

Remote Authentication Dial-In User Service (RADIUS)

- autentizuje klienty připojující se na NAS
  - přes WiFi, Ethernet s 802.1x, dial-in, ...
- Generický s ohledem na různé metody autentizace
  - jméno/heslo CHAP, certifikáty, ...
- Podpora účtování – informace o zahájení a ukončení relace
- Mohou fungovat i v proxy režimu
  - viz např. EduROAM
- Nad UDP/1812 (autentizace) UDP/1813 (účtování)
- RFC 2865 + 2866 (Accounting)

Lightweight Directory Access Protocol (LDAP)

- protokol pro ukládání a přístup k datům na adresářovém serveru
  - vychází z CCITT X.500
- smyslem je centralizace informací o uživatelích sítě
- stromová struktura objektů s různými atributy
  - hierarchický systém kontejnerů
- možnost modifikace schematu objektových tříd a jejich atributů

Pokročilé směrování

Směrování na “páteři” Internetu

- Existuje “páteř” Internetu ?
- Pojem autonomního systému
- Směrování mezi AS
  - BGP, princip path-vector
  - tranzitní a netranzitní AS
  - politiky směrování - atributy

Skupinové vysílání (multicasting)

- Smysl multicastingu
- Multicasting na LAN
  - multicast MAC adresy
  - podpora multicastingu v přepínačích
- Multicasting na WAN
  - distribuční stromy
  - PIM-SM

Kvalita služby - QoS

- Potřeba QoS
  - interaktivní aplikace, multimédia, VoIP, garantovaná odezva, ...
- QoS na LAN a na WAN
- Modely QoS
  - Integrated Services
    - RSVP
  - Differentiated Services
    - třídy provozu
    - značkování (implementace v IPv4, IPv6 a 802.1p)
- Zajištění QoS
  - různé režimy front, umělá fragmentace, regulace zpětné vazby v TCP

IP verze 6

- Motivace
- Adresace v IPv6
  - unicast, multicast, anycast (ne broadcast)
  - zápis adres
- Hlavička paketu IPv6, řetězení hlaviček
- Rozšíření v DNS, DHCP
- Současný stav implementace
  - OS, síťové prvky
- Koexistence IPv6 a Ipv4
- Integrovaná bezpečnost a mobilita

Mobile IP

- Udržení IP adresy při roamingu
  - Mobilní servery s pevnou veřejnou IP adresou
  - udržení navázaných relací během roamingu
  - průchod ACL
- Home agent a trojúhelníkové směrování
- Podpora MoIP v OS mobilních uzlů