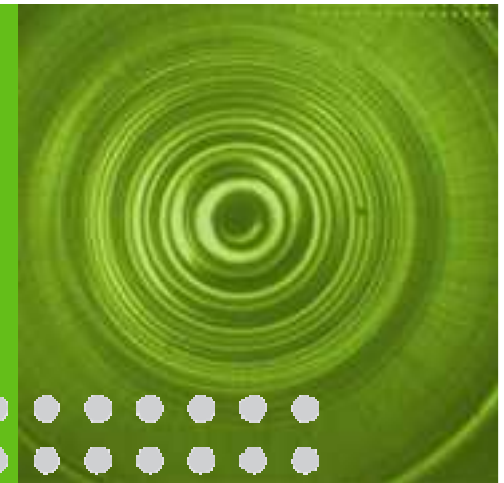


Principy a použití dohledových systémů



Ing. Tomáš Látal, tomas.latal@alcatel-lucent.com

23. listopadu 2010

Agenda

1. Proč používat síťový dohled
2. Úkoly zajišťované síťovým dohledem
3. Protokol SNMP
4. Autodiscovery - rozpoznání topologie sítě
5. Nástroje pro kontrolu SLA (Service Level Agreement)
6. Praktická ukázka



1

Proč používat síťový dohled

Důvody zavádění síťového dohledu

Potřebuji:

- Konfigurovat a spravovat síťové služby
- Kontrolovat funkci zařízení, sítě a služeb
- Sledovat kvalitu a dostupnost služeb
- Rychle odhalovat a opravovat poruchy v síti



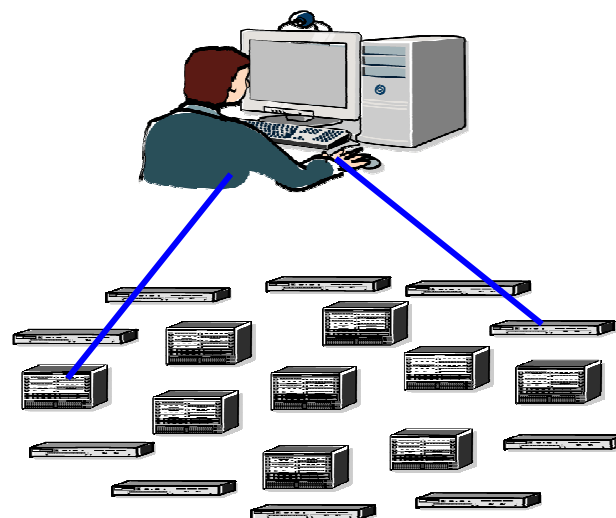
Sít' bez centrální správy

Použitelné pro:

- Malý počet zařízení
- Stabilní konfiguraci sítě - služby a zákazníci se příliš nemění

Konfigurace zařízení a služeb

- Uzel po uzlu
- Vysoká pravděpodobnost chyby
- Špatný přehled o síti jako celku



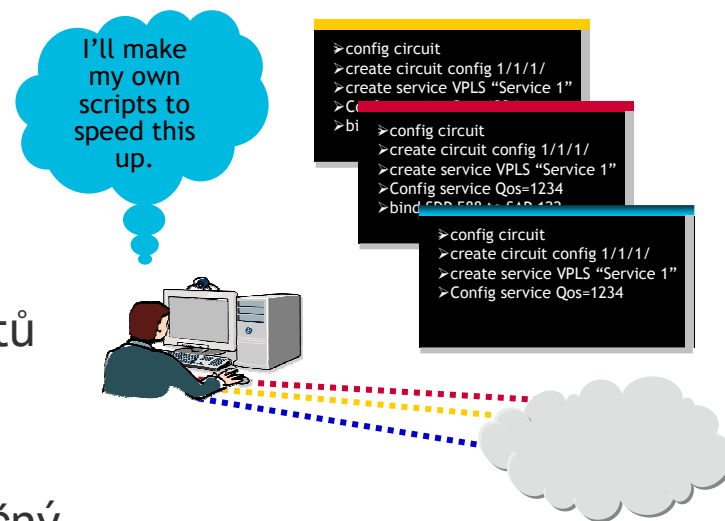
Správa sítě pomocí CLI skriptů

Výhody:

- Otevřené komunikační rozhraní
- Flexibilita
- Jednoduchá integrace se zastřešujícími systémy (OSS)
- Snadná integrace s externími databázemi

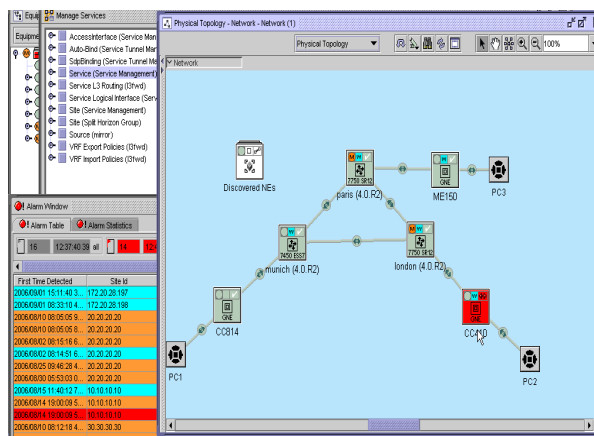
Nevýhody:

- Vyžaduje zaměstnance sběhlého v psaní skriptů
- Nezajistí snadný přehled o síti
- End-to-end service provisioning je velmi náročný
- Problematická správa alarmů



Správa sítě pomocí síťového dohledu - výhody

- Přehled o topologii sítě
- Přehled o stavech zařízení a linek v síti
- Přehledná správa alarmů, možnost jejich korelace
- Přehled o službách v síti, rychlá kontrola jejich konfigurace
- Snadné zavádění nových služeb



Správa sítě pomocí síťového dohledu - nevýhody

- Integrace se zastřešujícími systémy (OSS/BSS) může být náročnější
- Funkce vs. cena
- Určitá omezenost na správu sítě daného dodavatele dohledového systému
- Menší flexibilita v zavádění nových funkcí - čeká se zpravidla na novou verzi

Zamyšlení

- Potřebuji rychlý přehled o službách?
- Potřebuji urychlit obnovu služeb při poruše?
- Opravdu mám tak malou síť a přehled o službách, takže nepotřebuji dohled?
- Nemohl bych kvalifikované využít např. na rozvoj služeb místo ošetřování sítě?
- Pokud porostu, budu mít stále dost kvalifikovaných zaměstnanců a opravdu nebudu potřebovat přehled o síti a alarmech?
- Porovnání mzdových nákladů a ceny profesionálního softwaru
- Snížení mzdových nákladů vlivem menších nároků na kvalifikaci
- Cena integrace s mými systémy, podpora



2

Úkoly zajišťované
sítovým dohledem

Úkoly zajišťované síťovým dohledem

- Správa topologie sítě
- Správa služeb na úrovni služeb sítě
- Správa zákaznických služeb
- Kontrola stavů zařízení a okruhů v síti
- Kontrola SLA - Service Level Agreement
- Správa alarmů
- Odstraňování problémů v síti

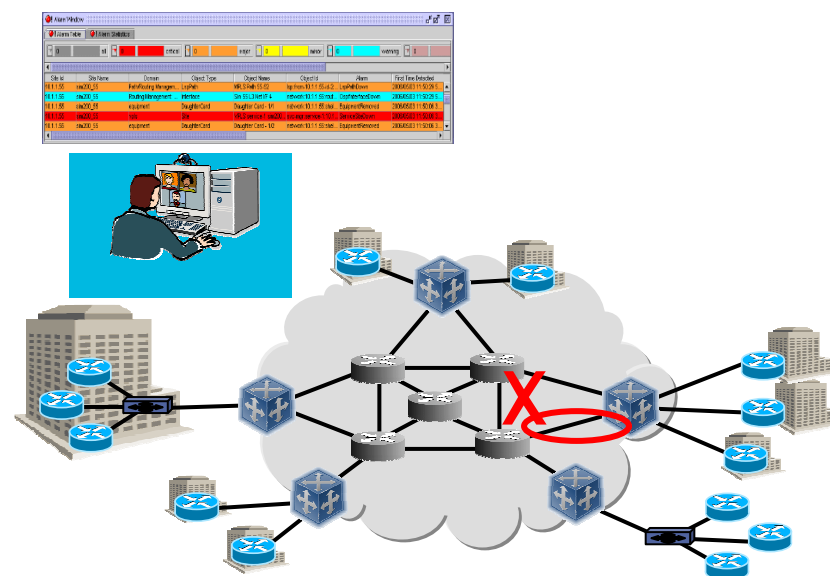
3

Protokol SNMP

Co je SNMP?

SNMP (Simple Network Management Protocol)

- protokol sloužící ke správě zařízení sítě
- založen na protokolu IP
- standardizován
- komunikace agent-manager



Verze protokolu SNMP

- SNMPv1
 - definice v RFC 1155, RFC 1156 (RFC 1213 - MIB-2), RFC 1157 (ietf.org)
 - komunikace založena na identifikátoru komunity
- SNMPv2
 - přidává nový typ přenášené zprávy PDU
 - definice v RFC 1441-1452
 - není zpětně kompatibilní s v1 kvůli odlišnému formátu PDU
 - používá se „ořezaná“ verze SNMPv2c (RFC 1901-1908)

Jak SNMPv1, tak SNMPv2 nedefinují mechanismy pro zabezpečení a autentizaci

Verze protokolu SNMP - pokračování

- SNMPv3
 - definice v RFC 3411-3418
 - zahrnuje šifrovací a autentizační mechanismy
 - kontroluje integritu zprávy
 - stále najdeme zařízení, která jej nepodporují

Metody zabezpečení SNMPv1/v2

- filtrace oprávněných IP adres
- směrování provozu důvěryhodnou, zabezpečenou sítí
- regulace podpory SNMP v jednotlivých zařízeních

Funkce SNMP - Typy PDU

get-request - dohled k uzlu: získání hodnoty proměnné (-ných)

get-next-request - dohled k uzlu: zjištění proměnných a jejich hodnot

get-response - uzel k dohledu: potvrzení

set-request - dohled k uzlu: požadavek na nastavení proměnné

trap - uzel k dohledu: upozornění dohledu uzlem na nějakou skutečnost, např. alarm, změna stavu portu, atp.

inform-request - dohled k dohledu, novinka v SNMPv2, podobné trapu

get-bulk-request - optimalizovaná verze GetNextRequest, novinka v SNMPv2

SNMP - MIB tabulka

- MIB = Management Information Base
- Definuje funkce podporované daným zařízením
- hierarchická stromová struktura

Příklad:

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime

- Je reprezentován číselnou kombinací v jednotlivých úrovních .1.3.6.1.2.1.1.3
- Jedná se o tzv. identifikátor objektu (OID, neboli ObjectID)

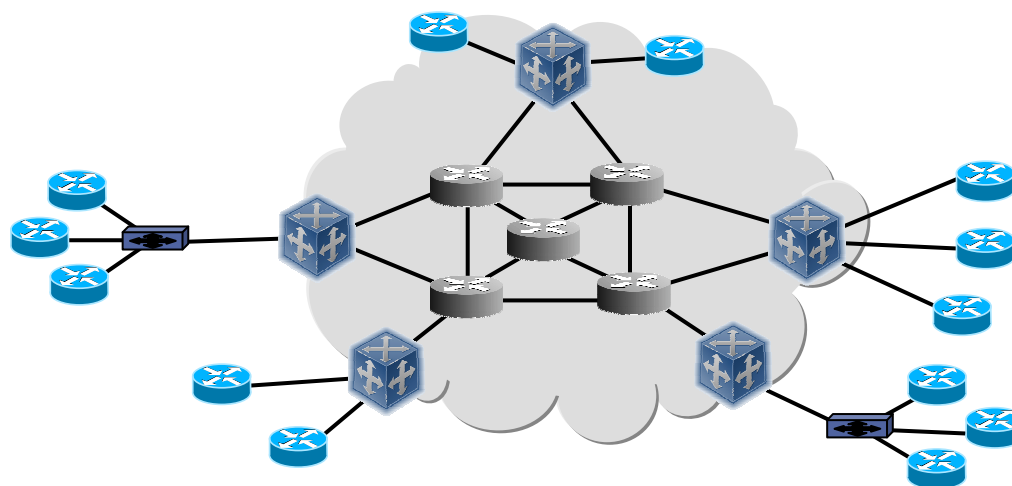
4

Autodiscovery

rozpoznání topologie sítě

Princip protokolů pro rozpoznání topologie sítě

- Výměna informací mezi síťovými prvky
- Informační pole zprávy obsahují informace týkající se např. jména prvků, nastavení fyzických rozhraní, apod.



Používané autodiscovery protokoly

- CDP - Cisco Discovery Protocol
- LLDP - Link Layer Discovery Protocol
- další proprietární protokoly

Cisco Discovery Protocol

- Každých 60s posílá zprávu na ethernetovou multicastovou adresu

01-00-0c-cc-cc-cc

- Informace zahrnuje např.:
 - verzi operačního systému
 - hostname (jméno prvku)
 - typ zařízení, model
 - nastavení duplexu
 - native VLAN, atd.

Link Layer Discovery Protocol

- Jedná se o standardizovaný protokol (IEEE 802.1AB)
- Zprávy posílá na ethernetovou multicastovou adresu

01-80-C2-00-00-0E

- Informace zahrnuje např.:
 - Systémové jméno a popis
 - Název portu a popis
 - VLAN name
- Adresu síťového dohledu
 - Systémové funkce (switching, routing, atp.)
 - Informace MAC/PHY
 - MDI power - Power over Ethernet
 - Link aggregation

5

Nástroje pro kontrolu SLA

Statistiky

Performance statistiky

- kontrola zatížení systému na fyzické úrovni
- odhalování problémů se zařízením

Např.: Počet vadných ethernetových rámců na rozhraní

Accounting statistiky

- přehled o konkrétních službách, resp. zákaznících
- přehled o konkrétních tocích v páteřní síti

Např.: přehled o QoS konkrétního zákazníka - pakety mimo profil, zahozené pakety z důvodu přetížení služby, atp.

Netflow (Cflowd)

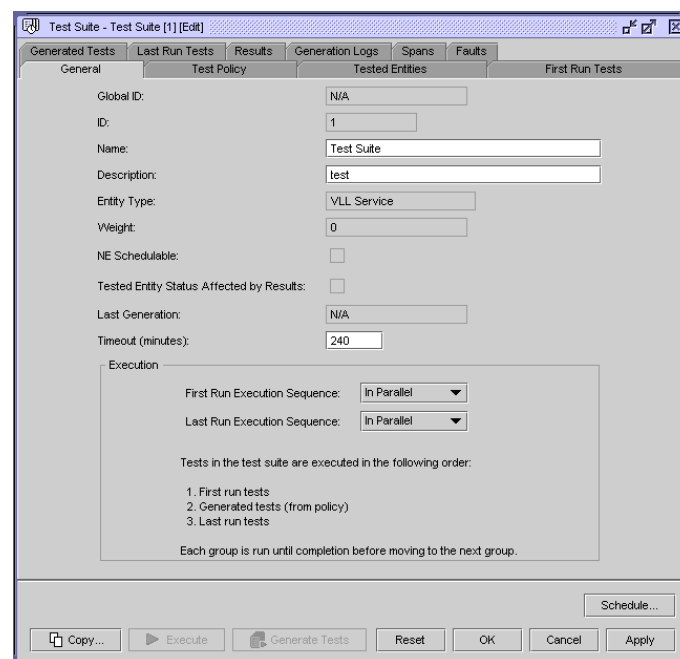
- Podobné informace jako Accounting statistiky
- Informace se zasílají na zvláštní prvek sítě Netflow collector - software zajišťující zpracování dat Netflow
- umožňuje vzorkování konkrétního toku a posílání výsledků na Netflow collector
- Lze definovat konkrétní sledovaný tok přes ACL (Access Control List), parametry mohou být TCP/UDP porty, IP adresy, TOS pole, atd.
- Zatěžuje směrovač

Netflow (Cflowd) - verze

- Verze 5 – Generuje fixní záznam pro každý individuální tok
- Verze 8 – Je schopna sloučit více individuálních toků do jednoho záznamu
- Verze 9 – Generuje variabilní exportní záznam v závislosti na konfiguraci zákazníka a typu vzokovaného toku např. IPv4 vs. MPLS. To provádí pro každý individuální tok

Service Test Manager

- Část dohledu MPLS sítě Alcatel-Lucent
- Umožňuje naplánovat spouštění různých testů
- Je možný export výsledků
- Umí vygenerovat alarm při překročení nastavených prahů



6

Praktická ukázka



Děkuji za pozornost

