Gerência de redes básica para pequenos provedores

Liane Margarida Rockenbach Tarouco
Leandro Marcio Bertholdo
Cesar Loureiro

RNP POP/RS

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

UFRGS
UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

Universiteit Twente
de ondernemende universiteit

INSTITUTO FEDERAL
Rio Grande do Sul
Campus Porto Alegre

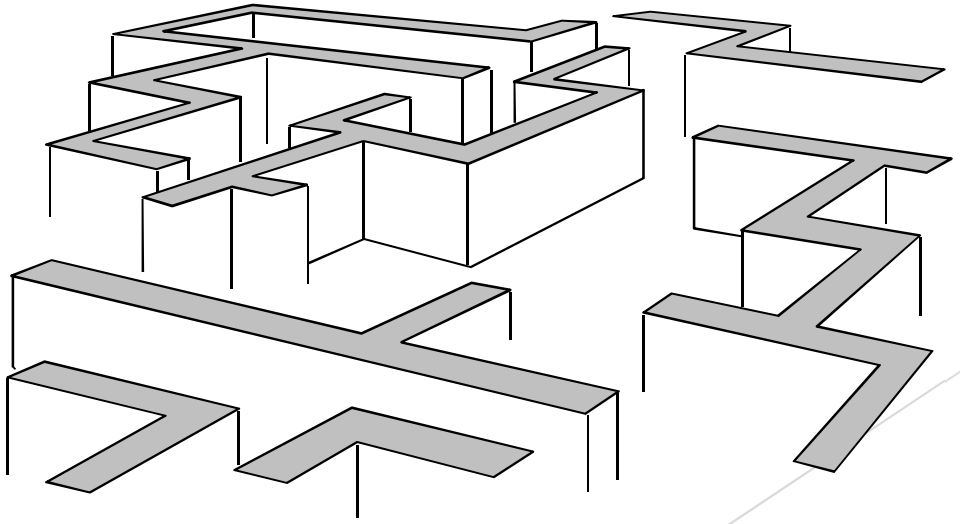
Tópicos

- FCAPS
  - Fault
  - Configuration
  - Accounting
  - Performance
  - Security

Escopo do gerenciamento

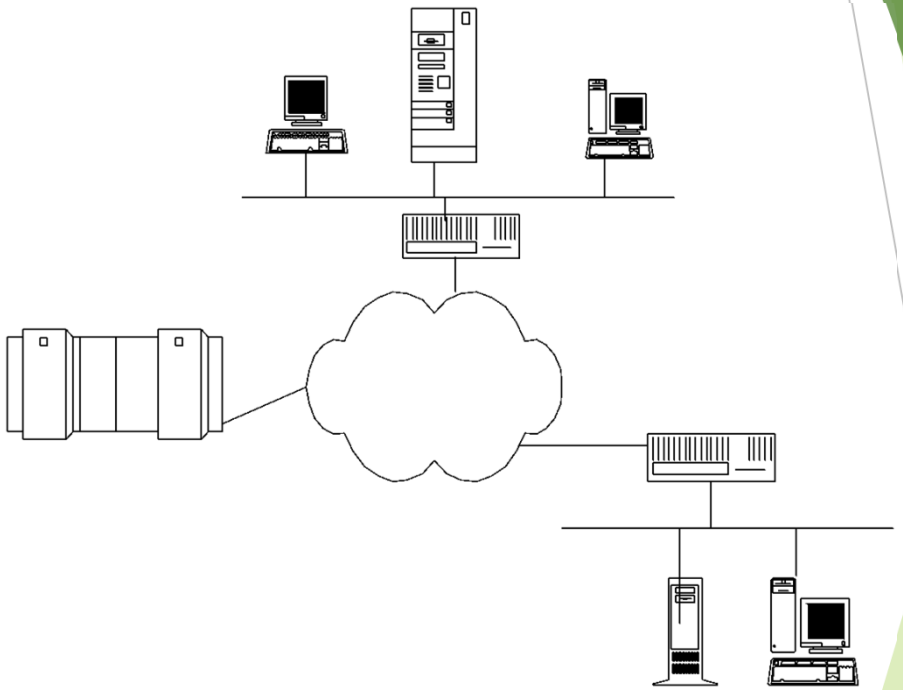
Gerência de problemas

- Descobrir os problemas
- Isolar, diagnosticar
- Manutenção



Isolando o problema

- Quem reportou
- Onde está conectado
- Componentes intermediários



Gerência de falhas

- Engloba
  - detecção,
  - isolação
  - correção de falhas

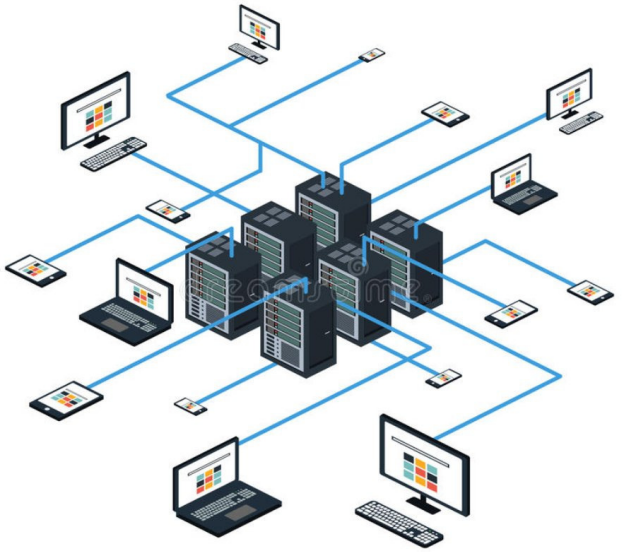
- Funções que só podem ser realizadas a partir da adição de valor aos dados brutos coletados da planta.

Dificuldades

- Dificuldade de obtenção de informações relevantes
- Excesso de informações básicas (contadores e indicadores de status)
- Interpretar e correlacionar os dados?

Causas das dificuldades

- Número crescente de equipamentos
- Muitos fornecedores com diferentes protocolos
- Muitos níveis de pessoal envolvido
- Diversas formas de controle e monitoração usadas nos diversos equipamentos com ferramentas próprias
- Falta de acesso direto a todos os componentes da rede para inspecionar e monitorar



Protocolo SNMP e MIB

- Agentes disponíveis em muitos tipos de equipamentos (HUBs, bridges, roteadores, estações UNIX, servidores de rede etc...)

Versões SNMP e MIB

- SNMP - versões
  - SNMP v2
- O conceito de MIB - Management Information Base
  - MIB 2 - gerenciamento hierárquico
  - MIBs proprietárias
  - RMON - gerenciar entidades sem agente SNMP

udpInDatagrams.

```
udpInDatagrams OBJECT-TYPE
               SYNTAX Counter
               Access read-only
               STATUS mandatory
               DESCRIPTION
                 "The total number of UDP datagrams
                  delivered to UDP users."
               ::= {udp 1}
```

Excesso de informações

- Para uma planta de telecomunicações típica o problema relacionado à carência de informações no centro de gerência de rede está gradativamente perdendo relevância.
- De fato, com o crescimento da planta gerenciada, associado à implantação de modelos de gerência, está havendo um grande aumento no volume de informações recebidas nos centros de gerência, tornando praticamente inviável o processamento "manual" de todas elas

Correlação de alarmes

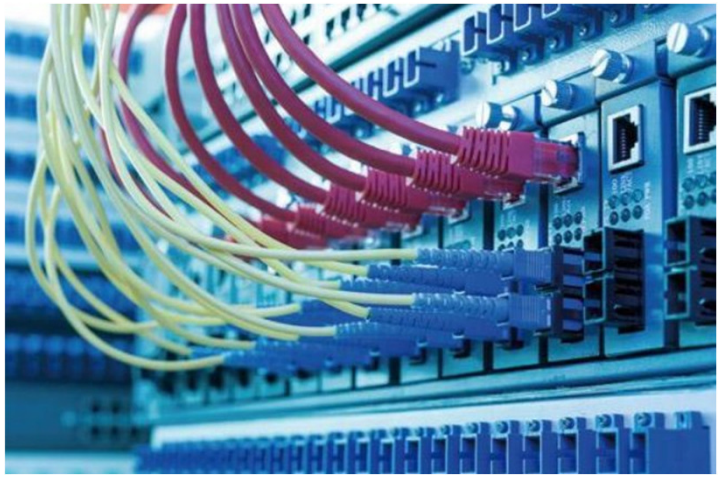
- Correlação de alarmes consiste na interpretação conceitual de múltiplos alarmes, resultando na atribuição de um novo significado aos alarmes originais
- Como parte do processo de correlação, dados brutos são interpretados e analisados, levando em consideração um conjunto de critérios pré-estabelecidos, ou definidos dinamicamente em função do processo de gerência.

Objetivo da correlação de alarmes

- A correlação geralmente tem como objetivo reduzir a quantidade de notificações de alarmes transferidas aos operadores do sistema de gerência de rede, aumentando o conteúdo semântico das notificações resultantes.

Alarme

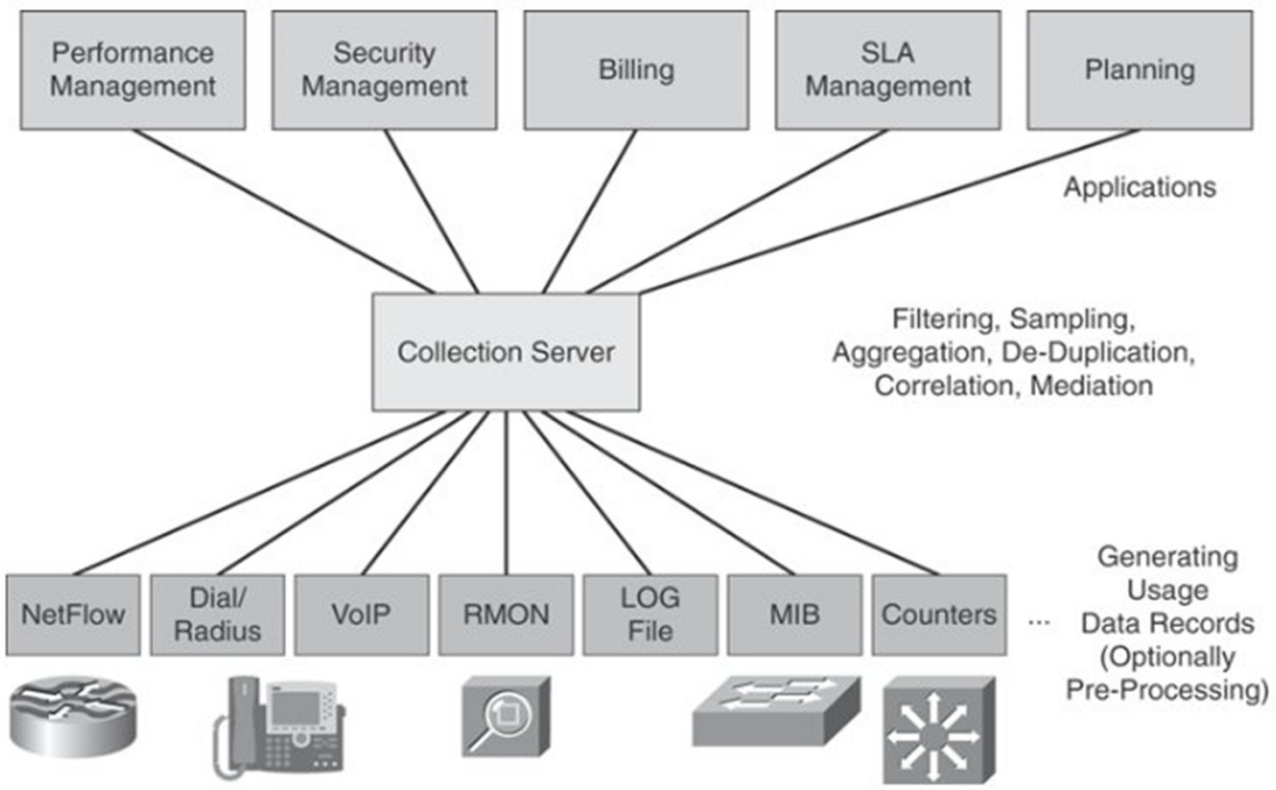
- Um alarme consiste de uma notificação sobre a ocorrência de um evento específico, que pode ou não representar um erro.
- Um relatório de alarme é um tipo de relatório de evento, usado no transporte de informações de alarme



Gerência de contabilização e performance

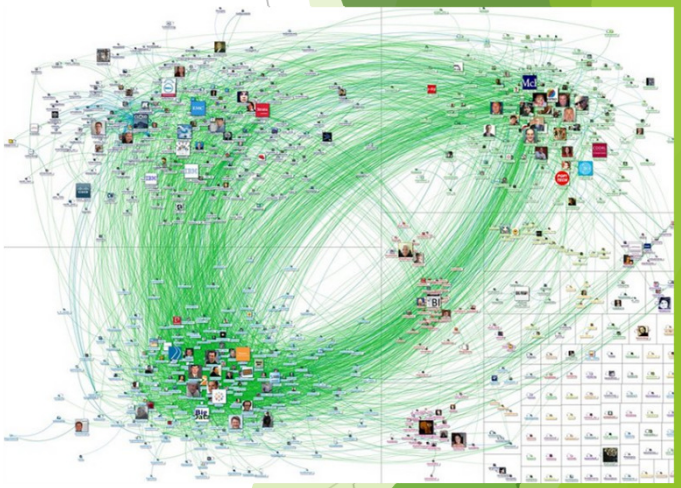
- Qual é a relação entre a contabilidade e gerência de performance?
- Por que redes exigem contabilidade e gerência de performance?
- Quais problemas que soluções de contabilidade e de gerência de performance resolver?
- Como pode o negócio usar essa informação para o planejamento da rede, redesenho e faturamento?
- Que aspectos compõem contabilidade e monitoramento de performance (coleta de dados, análise de dados, elaboração de relatórios, faturamento e assim por diante)?

Arquitetura para gerenciamento de contabilização



Registros de contabilização de acesso

- Quais aplicações geram a maior parte do tráfego
- Quais usuários utilizam estas aplicações
- Que % do tráfego elas representam
- Quantos usuários estão ativos na rede
- Quanto tempo os usuários permanecem ativos
- De onde eles acessam
- O que eles acessam
- Os usuários aceitam a política de uso da rede



Gerência de desempenho

- O monitoramento do desempenho coleta parâmetros relacionados com dispositivo, rede e serviços relatando os resultados via uma interface gráfica, arquivos de log etc
- A gerência do desempenho baseia-se nestas coletas de dados mas vai um passo além, notificando ativamente o administrador e reconfigurando os dispositivos, se necessário. Um exemplo é a coleta de dados para SLAs.
  - Analisar os dados e compará-la com limites predefinidos e definições de serviço.
  - Gerar trouble ticket para uma aplicação de gerência de problemas ou reconfigurar o dispositivo (filtrar o tráfego não prioritário ou aumentar a taxa de reserva de banda)

Gerência de performance

- Monitoração de performance - Coleta de atividades de rede no nível do dispositivo para fins de:
  - Monitoramento de desempenho relacionados com o dispositivo
  - Monitoramento de desempenho de rede
  - Monitoramento de desempenho de serviço
- Subtarefas de monitoramento incluem:
  - Monitoramento de disponibilidade
  - Tempo de resposta
  - Monitoração de utilização (enlace, dispositivo, CPU, rede, serviço etc...)
  - Assegurar precisão dos dados coletados
  - Verificação dos parâmetros de qualidade de serviço
  - Agregação de dados

Gerência de performance

- Análise de dados - baseline
  - Caracterização do tráfego de rede e de dispositivos
  - Performance
  - Exceções
  - Análise de capacidade
  - Baseline
  - Previsão de tráfego

Gerência de performance

- Enquanto a monitoração apenas observa, o gerenciamento de performance modifica configuração de dispositivos
  - Assegurar cumprimento de SLA
  - Definir limiares
  - Enviar informações para aplicações de alto nível
  - Ajustar configurações
  - Verificação de qualidade

Planejamento de capacidade

- Questões para provedores
  - Qual ponto de acesso gera mais lucro
  - Quais pontos de acesso não são rentáveis e deveriam ser consolidados
  - Deveria haver disponibilidade reservada para usuário premium
  - Em que segmento o tráfego está diminuindo? Clientes foram perdidos? Motivo?
- Questões para departamento de TI de empresa
  - Quais departamentos estão crescendo mais rápido
  - Que enlaces demandarão upgrade em breve
  - Para quais departamentos a conectividade de rede é critica e portanto deveria ter alta disponibilidade

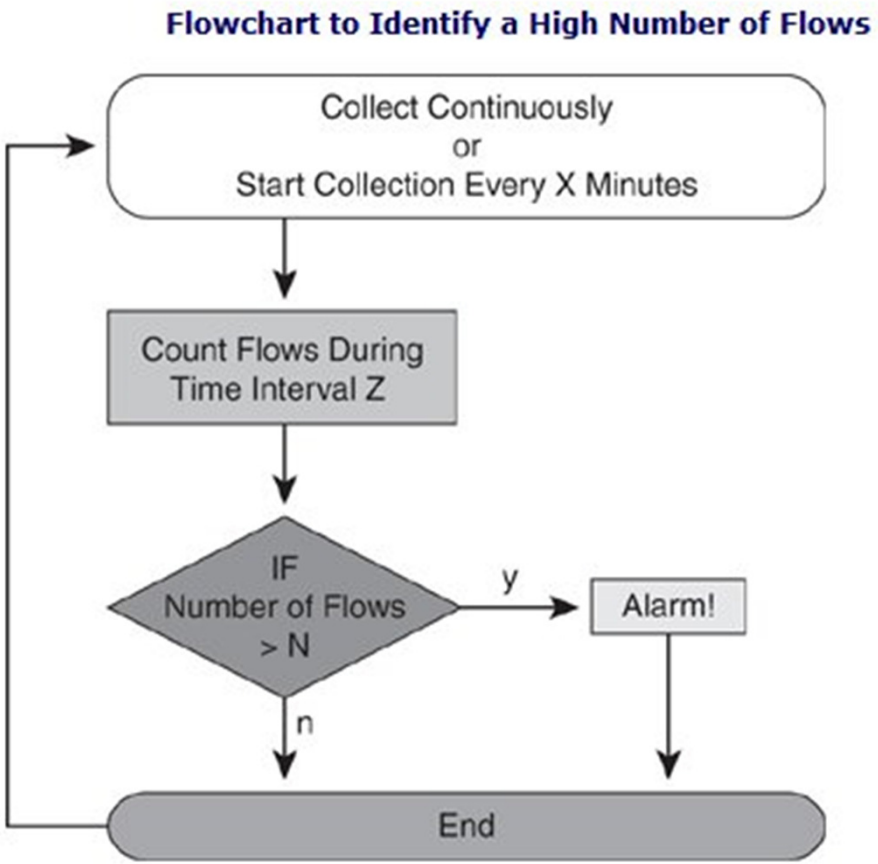
Questões que podem ser respondidas

- O que acontece se o tráfego de vídeos crescer 5% ao mês, constantemente ao longo do próximo ano
- Se o tráfego de voz aumentasse 10% ao ano, haveria gargalo? Onde
- Deve-se oferecer novos serviços?

Segurança

- Aumento súbito do tráfego total na rede
- Grande quantidade de tráfego inesperado gerado pelos hosts individuais
- Aumento do número de registros contábeis gerados.
- Vários registros contábeis com conteúdo anormal
- Uma alteração do mix de aplicações com um aumento súbito em aplicações "desconhecidas“
- Um aumento em certos tipos de tráfego e mensagens, como resets TCP ou mensagens ICMP
- Um número crescente de violações de regras das ACL (Access Control List)

Indícios derivados do número de fluxos



Identificando e bloqueando ataques

- Preparar a infra-estrutura de baseline e comparar parâmetros de segurança relevantes:

  - Monitorar dispositivos de rede

  - Identificar os principais parâmetros.

  - Armazenar estatísticas em um banco de dados.

  - Comparar os dados atuais com os valores armazenados.

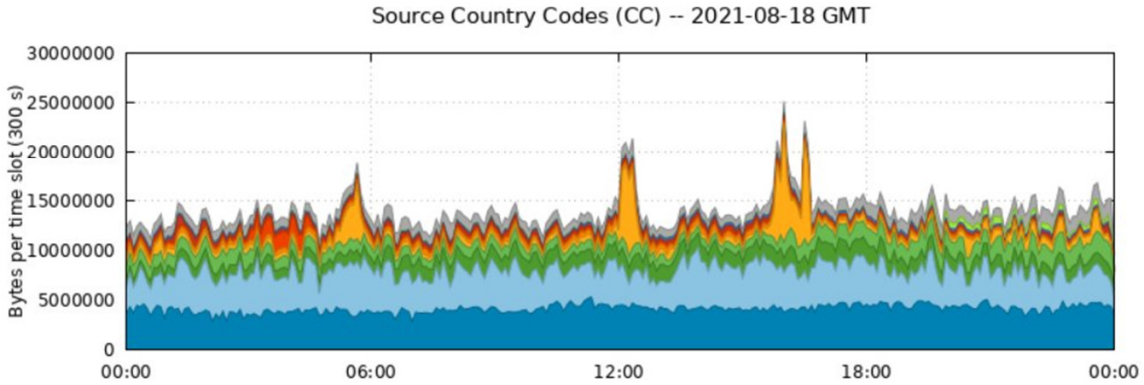
  - Gerar um evento se os limites forem ultrapassados ou desvios do normal potencialmente hostis são detectados.

Identificando e bloqueando ataques

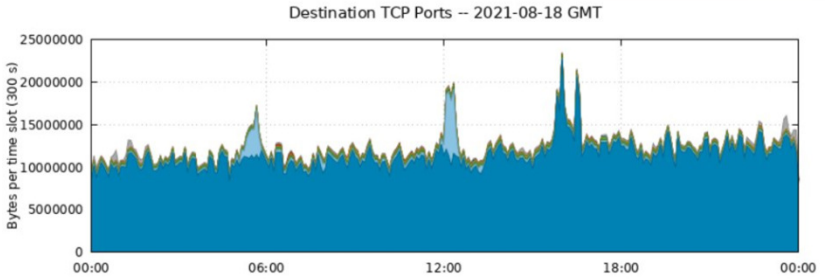
- Identificação
- Focalizar nos dispositivos envolvidos:
  - Quem é a vítima? Confira os fluxos para os maiores receptores de tráfego para identificar hosts comprometidos, o que é crucial em um ataque de negação de serviço distribuído.
  - Quais dispositivos de rede estão envolvidos? Monitorar os fluxos para identificar irregularidades.

Quem ataca?
Como ?

Source Country Codes (CCs)

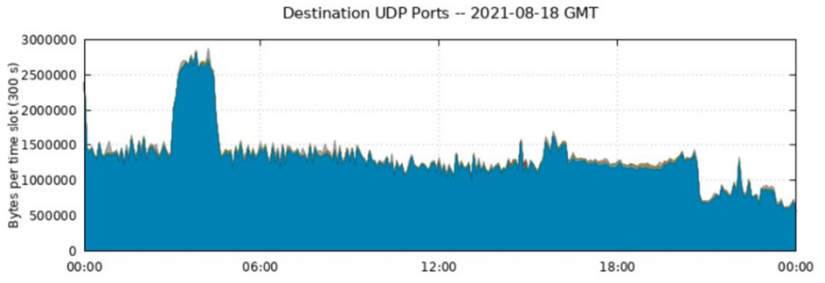


#	Key	CCs	Name	Total		Max	Avg
01		CN	China	1.19 GB	29.57 %	17.71 KB/s	13.75 KB/s
02		KR	Korea, The Republic of	1.11 GB	27.68 %	20.11 KB/s	12.87 KB/s
03		IN	India	390.95 MB	9.73 %	6.57 KB/s	4.52 KB/s
04		RU	Russian Federation	369.48 MB	9.19 %	7.70 KB/s	4.28 KB/s
05		US	United States of America	279.44 MB	6.95 %	40.54 KB/s	3.23 KB/s
06		AR	Argentina	101.79 MB	2.53 %	2.68 KB/s	1.18 KB/s
07		FR	France	88.24 MB	2.20 %	5.32 KB/s	1.02 KB/s
08		RO	Romania	70.30 MB	1.75 %	4.25 KB/s	813.69 B/s
09		BR	Brazil	69.41 MB	1.73 %	1.17 KB/s	803.40 B/s
10		TR	Turkey	47.98 MB	1.19 %	2.95 KB/s	555.35 B/s
11		Others		300.99 MB	7.49 %	10.29 KB/s	3.48 KB/s



#	Key	Port	Name	Total		Max	Avg
01		23	TELNET	3.26 GB	90.84 %	75.38 KB/s	37.72 KB/s
02		22	SSH (Secure Shell)	125.69 MB	3.50 %	25.35 KB/s	1.45 KB/s
03		3389	RDP (Microsoft Terminal Server)	60.60 MB	1.69 %	1.19 KB/s	701.38 B/s
04		445	Microsoft-DS Active Directory	32.05 MB	0.89 %	584.72 B/s	370.90 B/s
05		80	HTTP (Hypertext Transfer Protocol)	9.77 MB	0.27 %	1.43 KB/s	113.13 B/s
06		21	FTP (File Transfer Protocol - control)	7.86 MB	0.22 %	436.09 B/s	90.98 B/s

Destination UDP Ports



#	Key	Port	Name	Total		Max	Avg
01		5060	SIP (Session Initiation Protocol)	370.51 MB	96.32 %	9.38 KB/s	4.29 KB/s
02		123	NTP (Network Time Protocol)	2.15 MB	0.56 %	70.69 B/s	24.91 B/s
03		161	SNMP (Simple Network Management Protocol)	1.02 MB	0.26 %	78.86 B/s	11.77 B/s
04		53	DNS (Domain Name System)	742.41 KB	0.19 %	64.71 B/s	8.59 B/s

Gerência de rede

- Combinação de:
  - Equipamentos gerenciáveis
  - Sistemas de monitoração
  - Conhecimento
    - Conceitos
    - Topologia
    - Interpretação
  - Recursos humanos