Monitoramento e SIEM e NOC/SOC

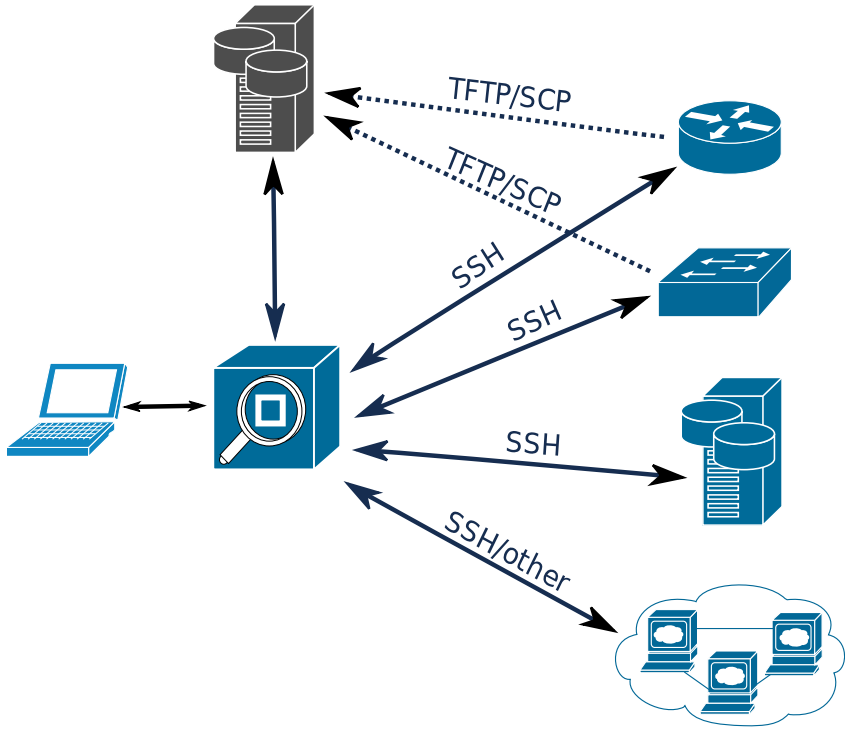
Segurança em Redes de Comunicações

Mestrado em Cibersegurança Mestrado em Engenharia de Computadores e Telemática
DETI-UA

universidade de aveiro
deti.ua.pt

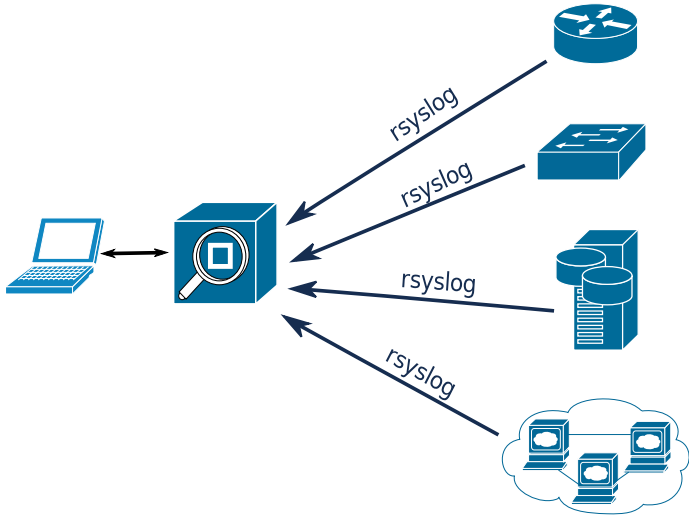
Acesso CLI remoto

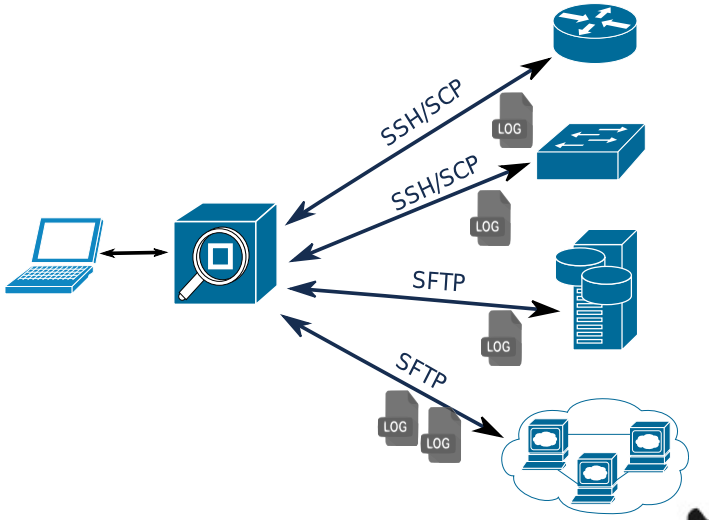
- Usando um console remoto para dispositivos,
  - Usando SSH, telnet (inseguro) ou protocolos proprietários,
  - Recuperar configurações e status de processos do dispositivo.
  - Os dispositivos também podem fazer upload de configurações para um ponto central.
    - Usando TFTP (inseguro) ou SFTP/SCP (muitos dispositivos não apoie).
- Envie “show” como comandos CLI, recupere a saída, analise informações.



Acesso aos arquivos de log

- rsyslog
  - Capaz de aceitar entradas de uma ampla variedade de serviços, transformá-los e enviar os resultados para diversos destinos de rede.
    - Sobre TCP e/ou SSL/TLS.
  - Temporização controlada pelo nó/ dispositivo monitorado.
  - Muitas tarefas de pós-processamento e processamento cruzado podem ser realizadas no monitorado nó/dispositivo.
- Acesso direto aos arquivos de log
  - Usando qualquer acesso remoto a arquivos remotos.
    - Requer permissões especiais.
  - SSH/SCP, SFTP, etc...
  - Temporização controlada por ponto central.
  - Requer todo o pós-processamento pesado e cruzado em um ponto central.

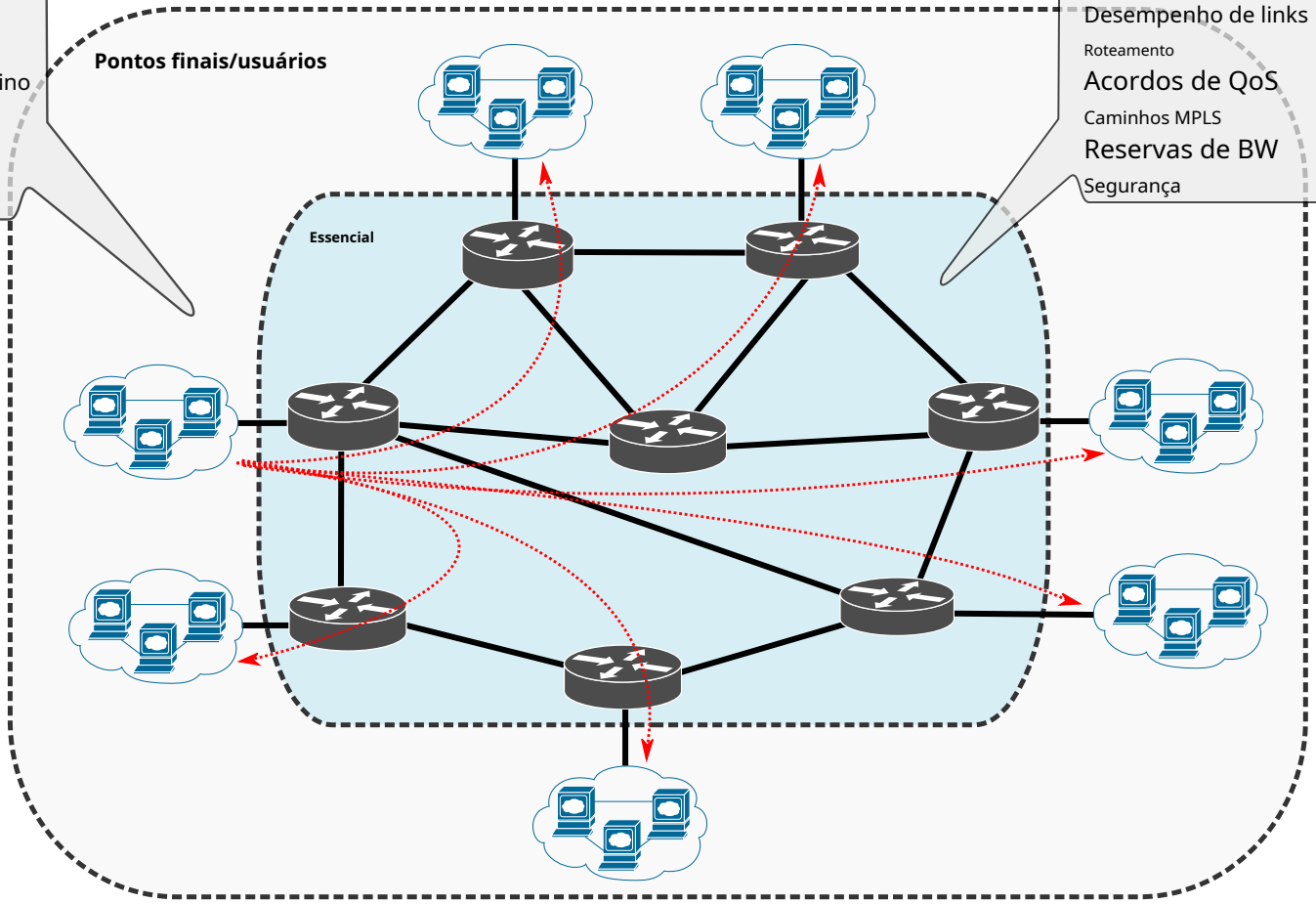




Monitoramento central e ponta a ponta

Medições ponta a ponta
- atraso
- nervosismo
- Taxa de transferência
- perdas
- Reservas BW
- validação de caminhos

reservados Demandas por destino
- global
- por serviço/aplicativo
- por uso de QoS



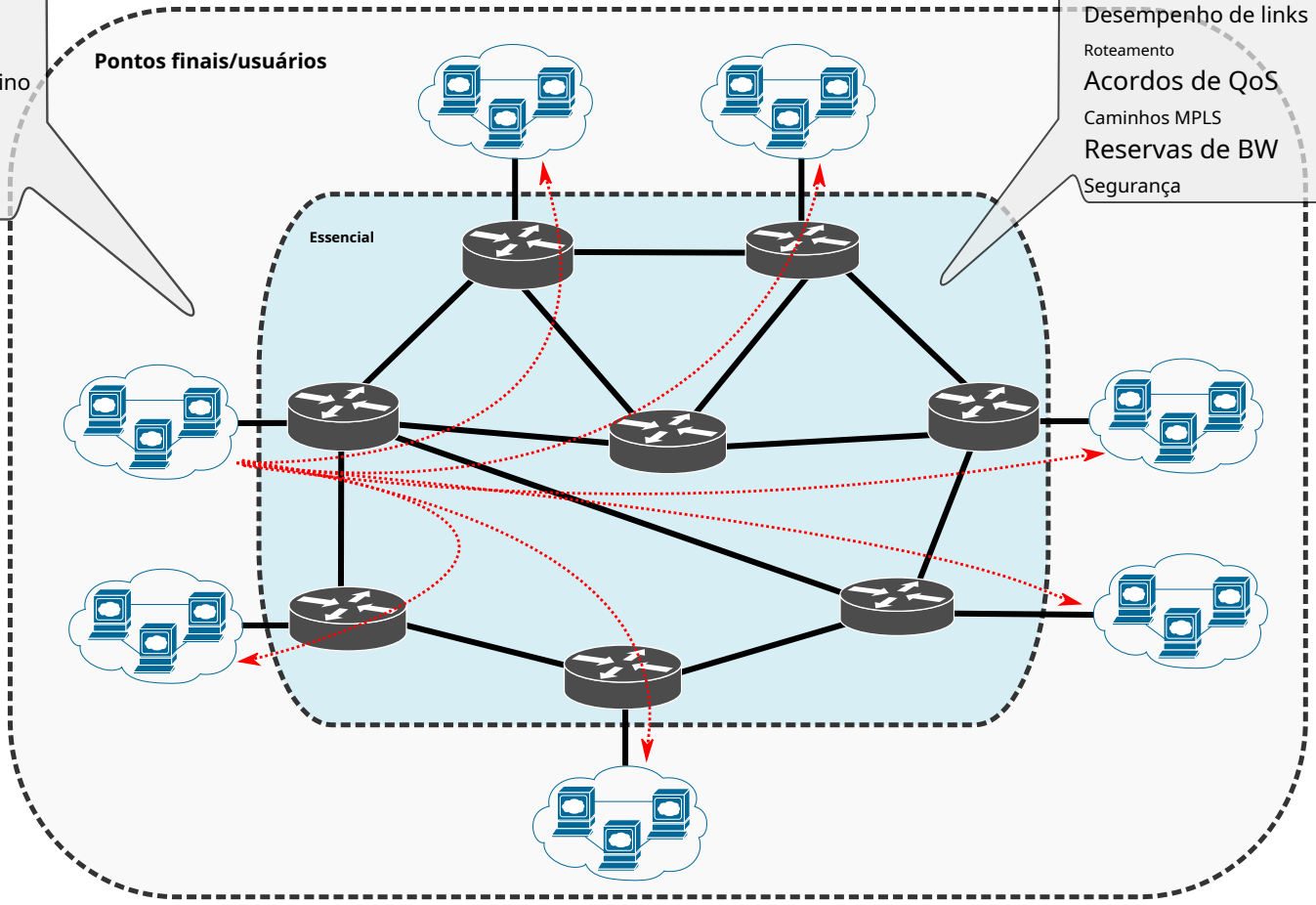
Configurações principais
- Consciência do nó
- Conscientização do serviço

Desempenho dos nós
Desempenho de links
Roteamento
Acordos de QoS
Caminhos MPLS
Reservas de BW
Segurança

Monitoramento central e ponta a ponta

Medições ponta a ponta
- atraso
- nervosismo
- Taxa de transferência
- perdas
- Reservas BW
- validação de caminhos

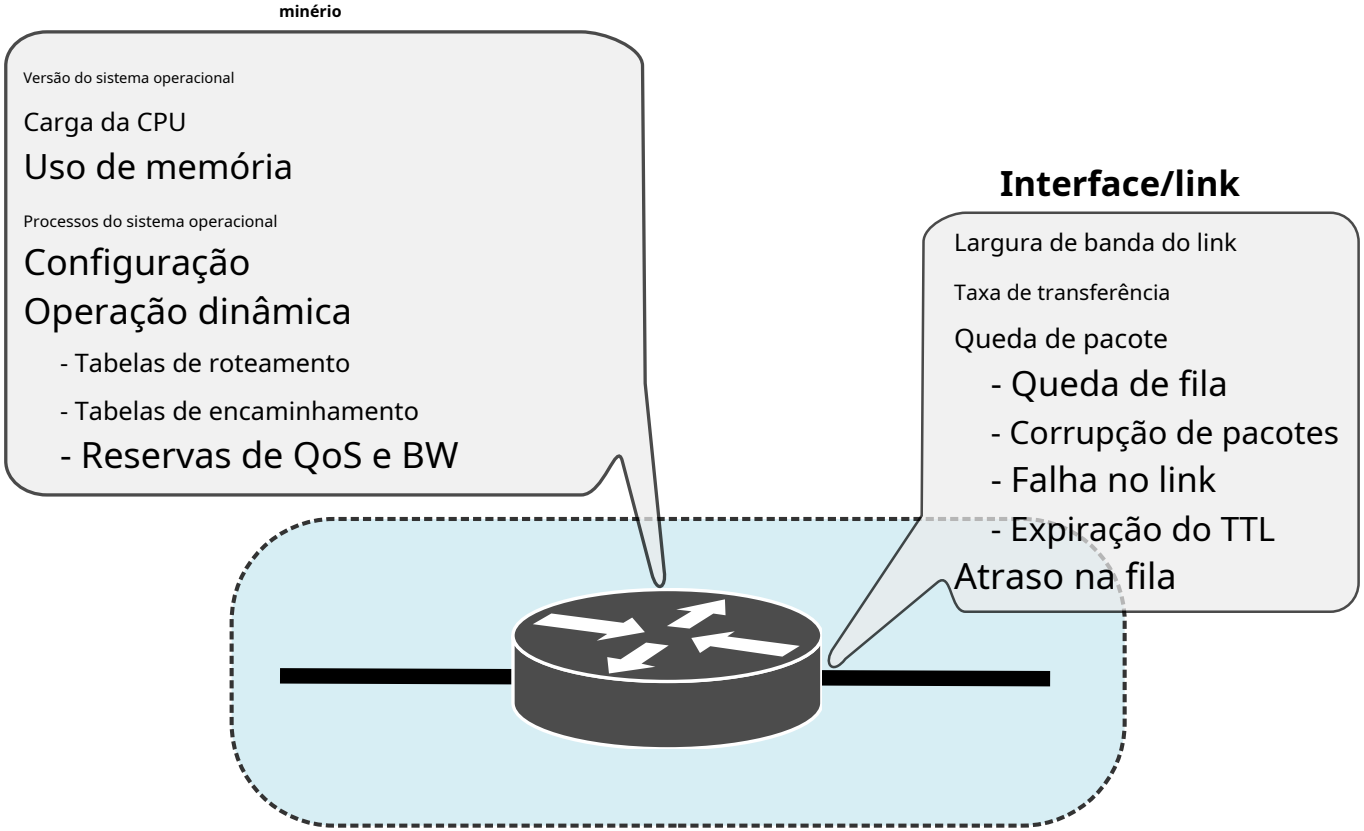
reservados Demandas por destino
- global
- por serviço/aplicativo
- por uso de QoS



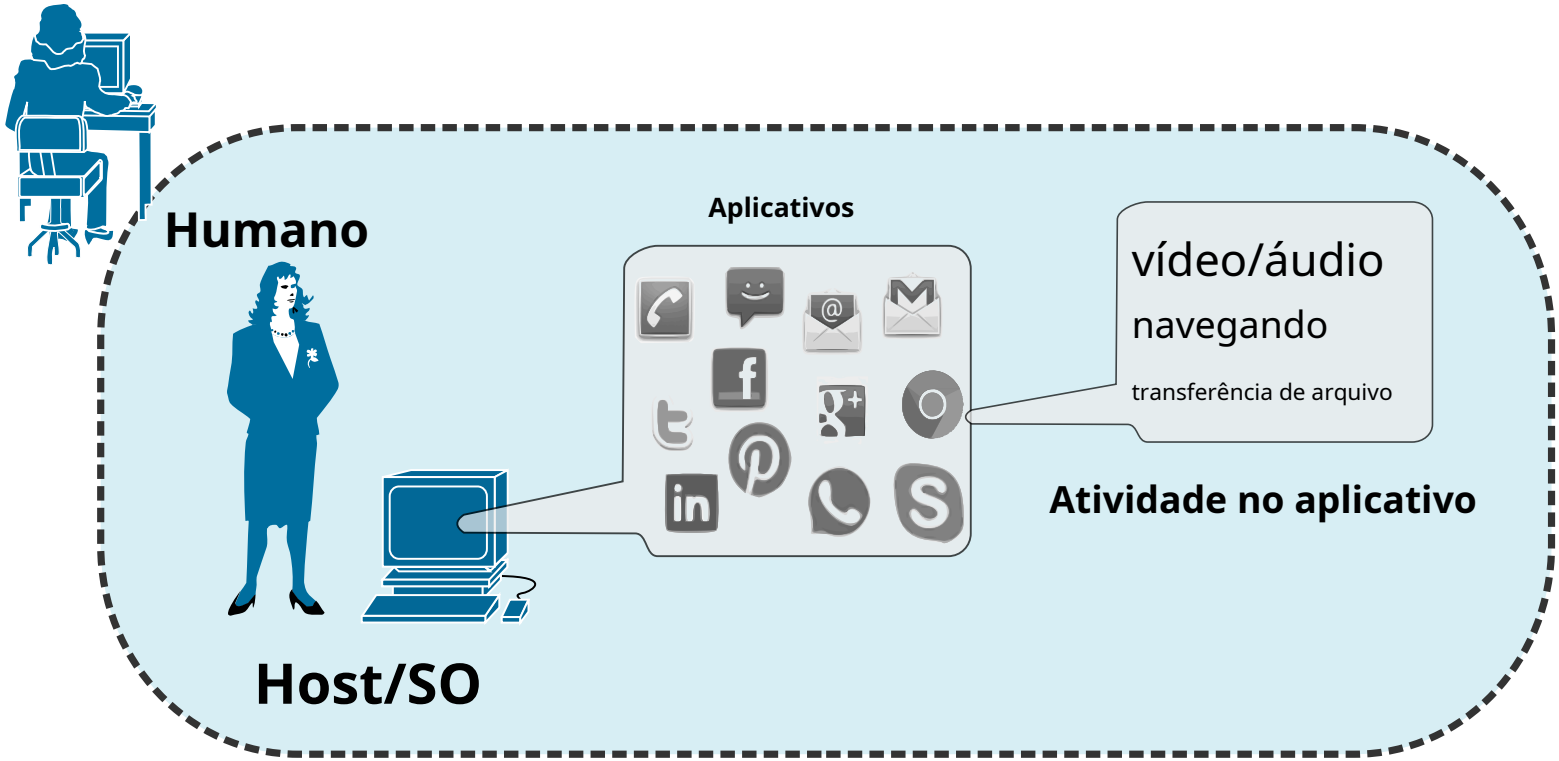
Configurações principais
- Consciência do nó
- Conscientização do serviço

Desempenho dos nós
Desempenho de links
Roteamento
Acordos de QoS
Caminhos MPLS
Reservas de BW
Segurança

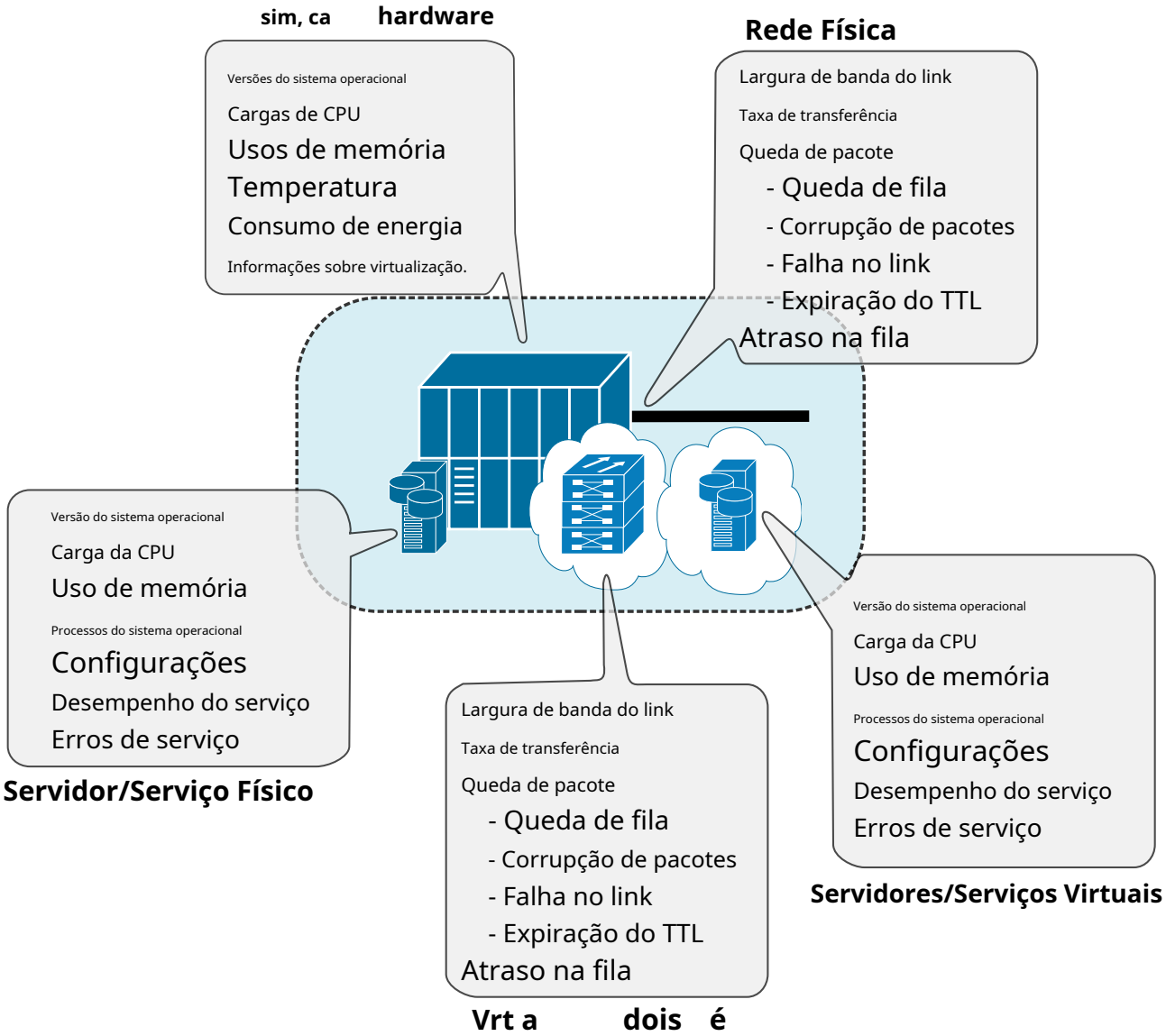
Monitoramento de nós



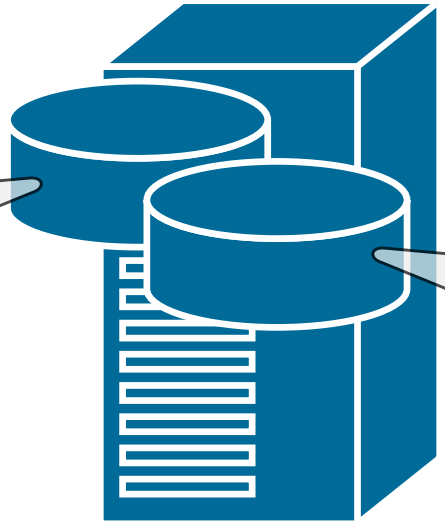
Monitoramento de usuário final/host/aplicativo



Monitoramento de servidor/serviço/nuvem



Monitoramento detalhado por serviço



Erros de serviço
Solicitações de clientes
ID/endereço do cliente
Respostas do servidor
Autenticação de objetos/ entradas acessadas
. . . .

Serviço A

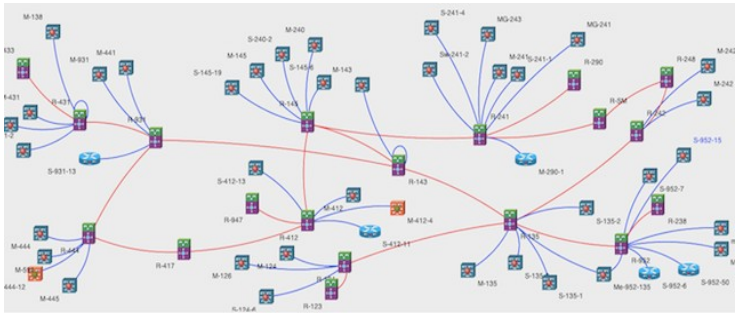
Erros de serviço
Solicitações de clientes
ID/endereço do cliente
Respostas do servidor
Uma autenticação de objetos/ entradas acessadas
. . . .

Serviço B

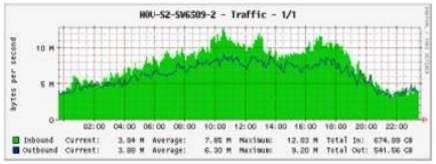
Fontes de dados

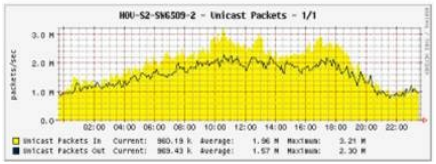
- SNMP
  - Usado para adquirir conhecimento sobre o estado atual de nós/links/servidores.
  - Informações locais. Pode ser usado para extrapolar para informações globais.
  - (Frequentemente) Requer o uso de MIBs específicos do fornecedor.
- Exportação de fluxo
  - Usado para caracterizar usuários/serviços em termos de quantidade de tráfego e destinos de tráfego.
  - Informações em escala temporal média e grande.
  - Protocolos: Cisco NetFlow, IPFIX – Standard, Juniper jFlow e sFlow
- Capturas de pacotes/estatísticas RAW/DPI vs. SPI
  - Usado para caracterizar usuários/serviços em pequenas escalas de
  - tempo. Requer probes dedicados distribuídos.
- Acesse logs de servidor/dispositivo e/ou acesso CLI.
  - Usado para adquirir conhecimento sobre o estado passado e atual.
- Medições ativas
  - Introduz entropia na rede e requer (para muitas medições) sincronização precisa do relógio
  - Por exemplo, atraso/jitter unidirecional, atraso/jitter de ida e volta.

SNMP



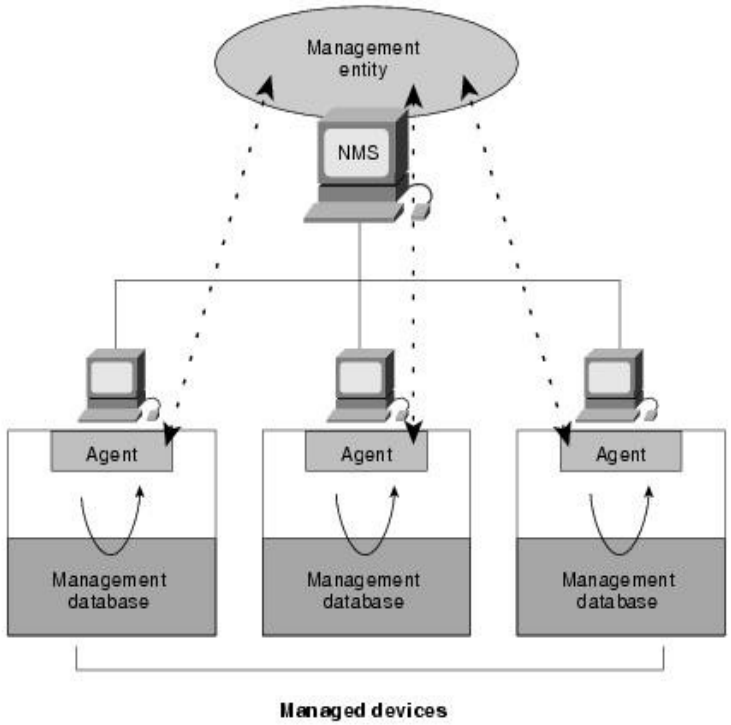
- Usado para adquirir o status e o uso de nós, links e serviços ao longo do tempo.
  - Requer extração periódica para obter informações ao longo do tempo.
- Usado para obter:
  - Elementos de rede e interconexões,
  - Serviços implantados em rede.
- Usado para estimar, caracterizar e prever:
  - Desempenho do fluxo de dados.
    - Perdas de pacotes e (por inferência indireta) atraso/jitter nos nós.
    - Permite obter informações sobre o desempenho atual e futuro do serviço
  - Desempenho dos nós,
    - Uso de memória/CPU, número de processos, etc...
    - Permite detectar pontos de falha, nós de degradação de serviço, nós instáveis.
  - Uso de link de rede,
    - Bytes de entrada/saída e contagens de pacotes.
    - Permite realizar otimizações em termos de roteamento (balanceamento de carga), upgrade de link e introdução de redundância.
  - Roteamento de dados/fluxo,
    - Nos níveis Camada 2, Camada 3 e MPLS.
    - Permite compreender como os dados fluem e como podem reagir a eventos disruptivos.





Componentes básicos do SNMP

- Uma rede gerenciada por SNMP consiste em três componentes principais:
- Dispositivos gerenciados
  - Nó de rede que contém um agente SNMP.
  - Colete e armazene informações de gerenciamento e disponibilize essas informações usando SNMP.
  - Podem ser roteadores e servidores de acesso, switches, pontes, hubs, hosts de computadores ou impressoras.
- Agentes
  - Módulo de software de gerenciamento de rede que reside em um dispositivo gerenciado.
- Sistemas de gerenciamento de rede (NMSs)
  - Executa aplicativos que monitoram e controlam dispositivos gerenciados.
  - Fornece a maior parte dos recursos de processamento e memória necessários para o gerenciamento de rede.
  - Um ou mais NMSs devem existir em qualquer rede gerenciada.

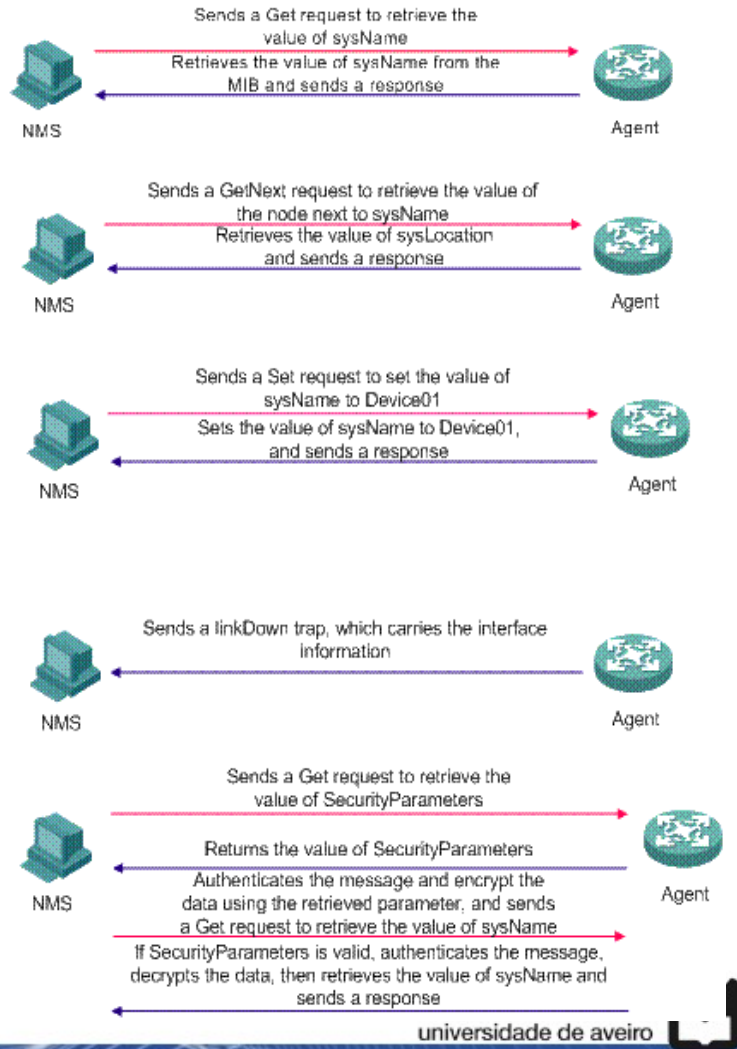


Versões SNMP

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithm.
v3	authPriv	MD5 or SHA	DES or AES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit or CFB128-AES-128 encryption in addition to authentication based on the CBC-DES (DES-56) standard.

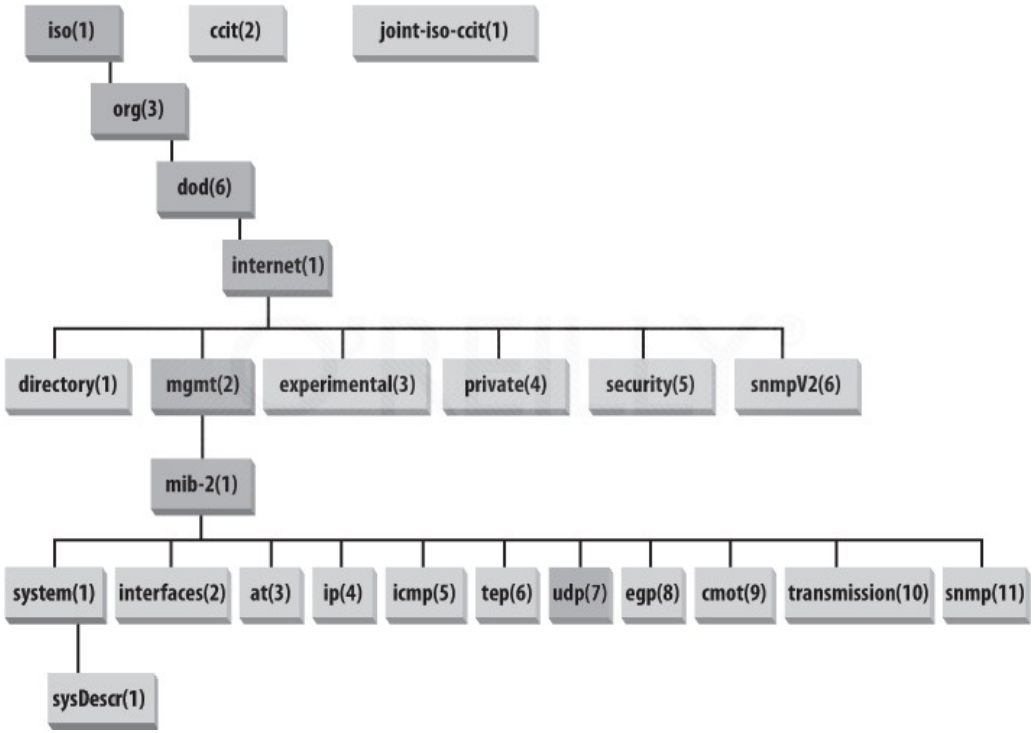
Operações SNMP

- O SNMP fornece as cinco operações básicas a seguir:
  - Obter operação
    - Solicitação enviada pelo NMS ao agente para recuperar um ou mais valores do agente.
  - Operação GetNext
    - Solicitação enviada pelo NMS para recuperar o valor do próximo OID da árvore.
  - Definir operação
    - Solicitação enviada pelo NMS ao agente para definir um ou mais valores do agente.
  - Operação de resposta
    - Resposta enviada pelo agente ao NMS.
  - Operação de armadilha
    - Resposta não solicitada enviada pelo agente para notificar o NMS dos eventos ocorridos.
- No SNMPv3, as operações get são realizadas usando autenticação e criptografia.



Módulos MIB e identificadores de objetos

- Um módulo SNMP MIB é uma especificação de informações de gerenciamento em um dispositivo
- O SMI representa a estrutura do banco de dados MIB em forma de árvore com tabelas conceituais, onde cada recurso gerenciado é representado por um objeto
- Identificadores de Objeto (OIDs) identificam ou nomeiam exclusivamente variáveis MIB na árvore
  - Sequência ordenada de inteiros não negativos escritos da esquerda para a direita, contendo pelo menos dois elementos
  - Para facilitar a interação humana, os nomes com valor de string também identificam os OIDs
    - MIB-II (ID do objeto 1.3.6.1.2.1)
    - MIB privado da Cisco (ID do objeto 1.3.6.1.4.1.9)
- A árvore MIB é extensível com novos módulos MIB padrão ou por ramos experimentais e privados
  - Os fornecedores podem definir suas próprias filiais privadas para incluir instâncias de seus próprios produtos



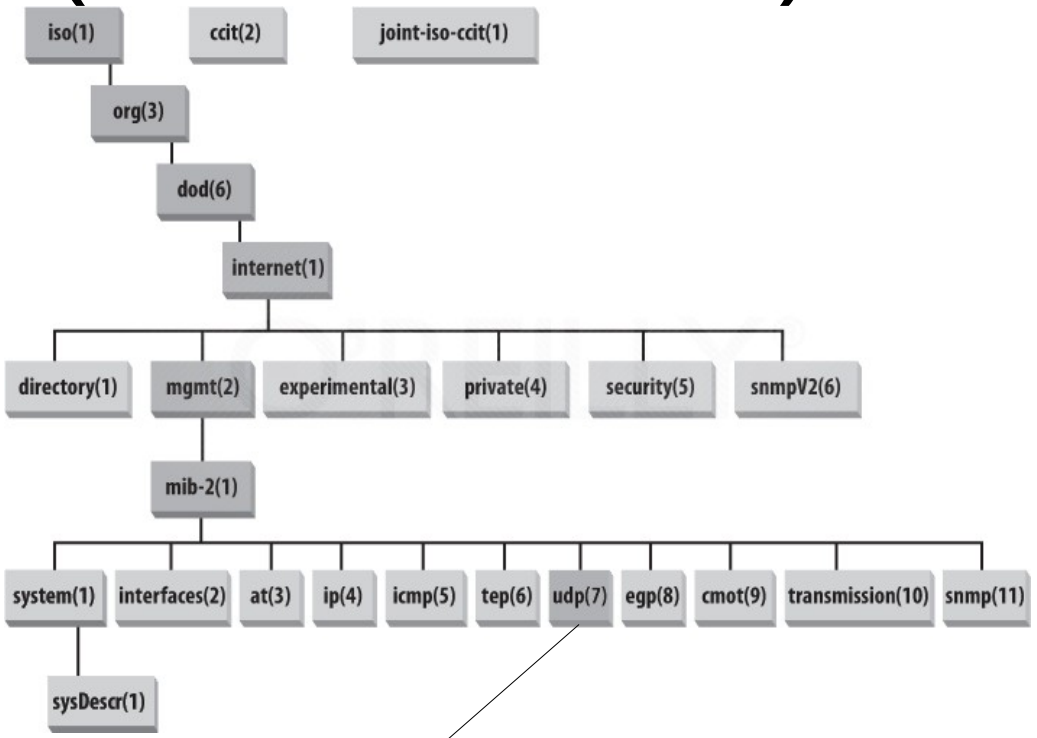
Nomes SNMP (números/OID)

- Para nomear todos objetos possíveis (protocolos, dados, etc.) é usado um ISO

  Identificador de objeto

  Árvore (OID):

  - Hierárquico nomenclatura de objetos
  - Cada folha da árvore tem um nome e número



1.3.6.1.2.1.7.1

ISO

Identidade ISO. Organização

Departamento de Defesa dos EUA

Internet

udpInDatagrams

UDP

MIB2

gerenciamento

universidade de aveiro

MIBs SNMP

- Management Information Base (MIB): conjunto de objetos gerenciados, utilizado para definir informações dos equipamentos, e criado pelo fabricante
- Exemplo: módulo UDP

ID do objeto	Nome	Tipo	Comentários
1.3.6.1.2.1.7.1	UDPInDatagramas	Counter32	Número de datagramas UDP entregues aos usuários.
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	Número de datagramas UDP recebidos para os quais não houve aplicação no porto de destino.
1.3.6.1.2.1.7.3	Erros UDPIn	Counter32	O número de UDP recebidos datagramas que não puderam ser entregues por outros motivos que não a falta de aplicação no porto de destino.
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	O número total de datagramas UDP enviado por esta entidade.

MIBs relevantes

- Características da interface, configurações, status e estatísticas:
  - IF-MIB e IP-MIB.
  - Informações adicionais da Cisco: CISCO-QUEUE-MIB, CISCO-IF-EXTENSION-MIB
- Informações de gerenciamento de nós (descrição, informações gerais, status da CPU/ memória, etc...):
  - SNMPv2-SMI e ENTITY-MIB.
  - Específico do fornecedor: CISCO-SMI, JUNIPER-SMI, etc...
  - Extras Cisco: CISCO-PROCESS-MIB, CISCO-FLASH-MIB, CISCO-ENVMON-MIB, CISCO-IMAGE-MIB, etc...
- Roteamento de nós e engenharia de tráfego:
  - IP-MIB, IP-FORWARD-MIB
    - Informações adicionais da Cisco: CISCO-CEF-MIB, CISCO-PIM-MIB
  - MPLS-TE-MIB, MPLS-LSR-MIB, MPLS-VPN-MIB
- Serviços de nó:
  - Específico do fornecedor: CISCO-AAA-SESSION-MIB, CISCO-SIP-UA-MIB, etc...
- Mecanismos de monitoramento de nós:
  - RMON-MIB, RMON2-MIB, CISCO-SYSLOG-MIB, CISCO-RTTMON-MIB, CISCO-NETFLOW-MIB, CISCO-IPSEC-FLOW-MONITOR-MIB, etc...

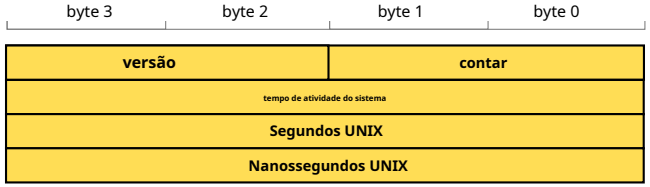
Fluxo de rede

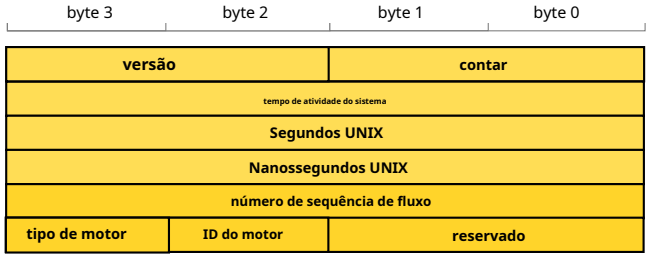
- Os serviços Cisco NetFlow fornecem aos administradores de rede informações de fluxo IP de suas redes de dados.
  - Os elementos da rede (roteadores e switches) coletam dados de fluxo e os exportam para
  - coletores. Captura dados de pacotes de entrada (entrada) e/ou saída (saída).
  - Coleta estatísticas para pacotes IP para IP e IP para MPLS.
- Um fluxo é definido como uma sequência unidirecional de pacotes com algumas propriedades comuns que passam por um dispositivo de rede.
  - Um fluxo é identificado como a combinação dos seguintes campos-chave:
    - Endereço IP de origem, Endereço IP de destino, Número da porta de origem, Número da porta de destino, Tipo de protocolo da Camada 3, Tipo de serviço (ToS) e Interface lógica de entrada.
- Esses fluxos coletados são exportados para um dispositivo externo, o coletor NetFlow.
- Os fluxos de rede são altamente granulares
  - Por exemplo, os registros de fluxo incluem detalhes como endereços IP, contagens de pacotes e bytes, carimbos de data/hora, tipo de serviço (ToS), portas de aplicativos, interfaces de entrada e saída, números de sistemas autônomos, etc.
- O NetFlow possui três versões principais: v1, v5 e v9.
  - v1 é recomendado apenas para dispositivos legados sem suporte para v5 ou
  - v9. V1 e v5 não suportam fluxos IPv6.

NetFlow versões 1 e 5

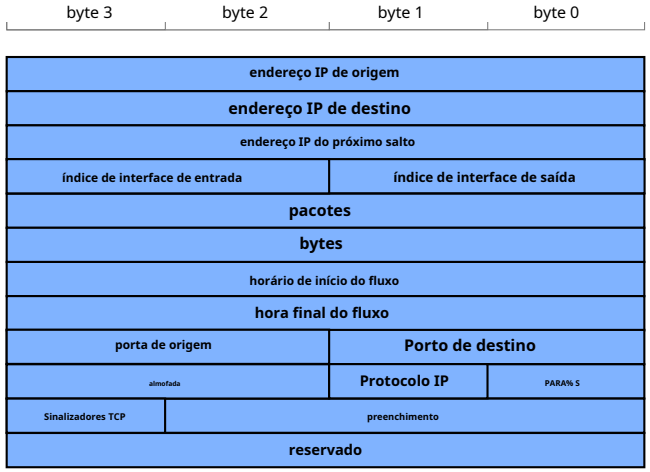
- Pacotes NetFlow v1/v5 são pacotes UDP/IP com um cabeçalho NetFlow e um ou mais registros de dados NetFlow

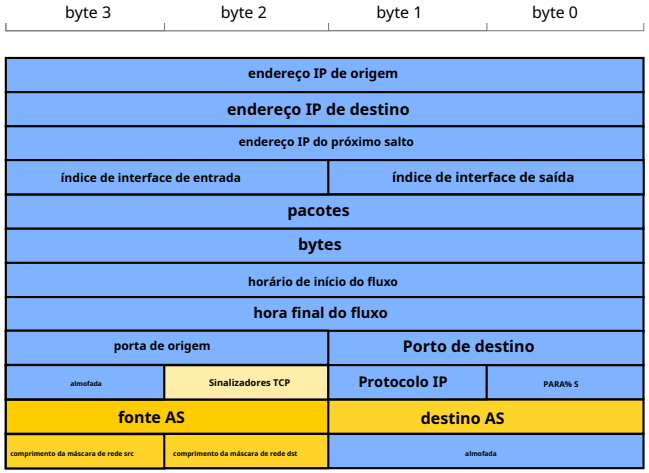
Cabeçalho formatar





Registro formatar



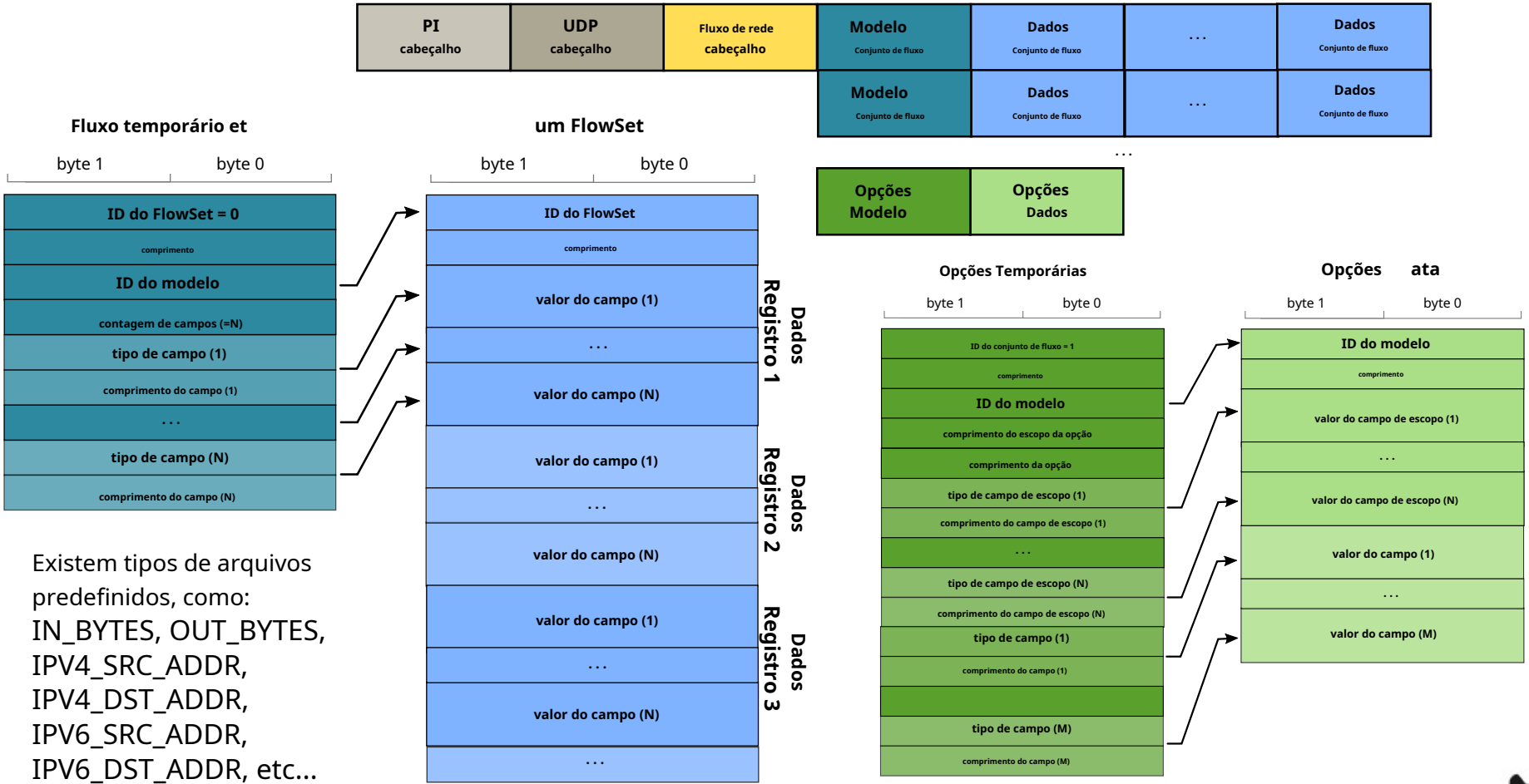


Versão 1

Versão 5

NetFlow versão 9

- Os pacotes NetFlow v9 são pacotes UDP/IP com um cabeçalho NetFlow, um ou mais Template FlowSets (podem ser suprimidos, se enviados anteriormente), um ou mais Data FlowSets e, opcionalmente, um Options Template e Data Record.



Existem tipos de arquivos predefinidos, como:
IN_BYTES, OUT_BYTES,
IPV4_SRC_ADDR,
IPV4_DST_ADDR,
IPV6_SRC_ADDR,
IPV6_DST_ADDR, etc...

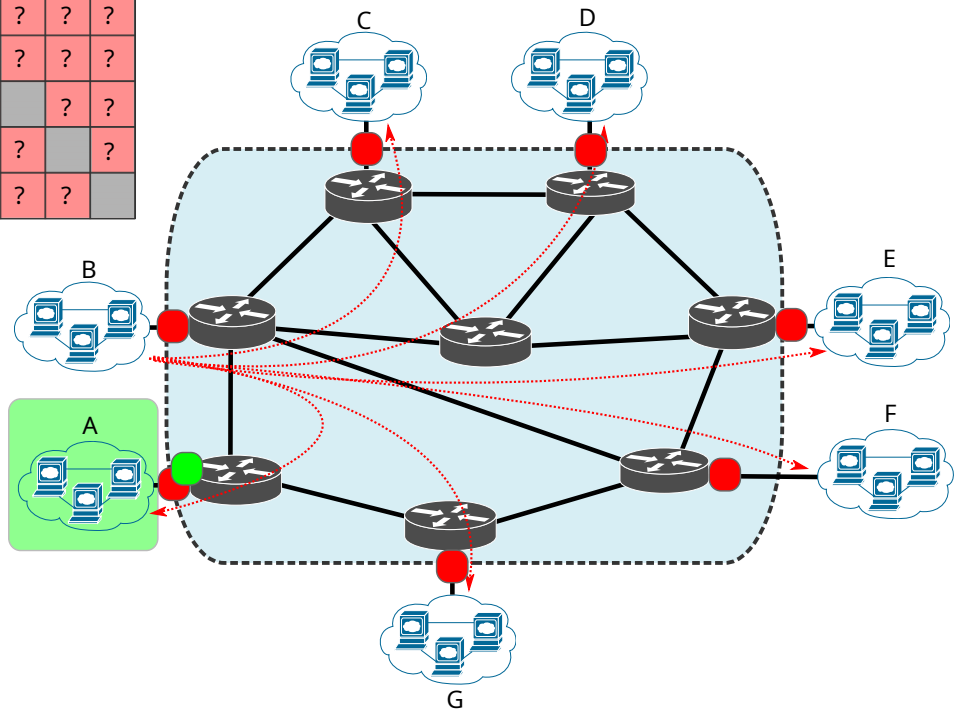
Uso do NetFlow

- Usado para caracterizar usuários/serviços em termos de quantidade de tráfego.
  - Usuários/Grupos (geral ou por aplicativo) → Aplicado em interfaces (V)LAN.
  - Serviços → Aplicado a interfaces de data center
- Usado para caracterizar destinos de tráfego (para pontos de saída) de um ponto de entrada específico em uma rede:matrizes de tráfego .
  - Os pontos de entrada/saída podem ser:
    - Links de acesso à rede (camada de distribuição L3SW, roteadores de acesso à Internet, links de servidor VPN do usuário),
    - Links de borda central de rede (roteadores de borda central),
    - links de peering BGP (roteadores AS Border).
- Usado para caracterizar o roteamento “na rede”.
  - Complexo de implementar e processar.

Implantação do NetFlow

- Interfaces para monitorar depende do objetivo:
  - Matriz de tráfego inferência – todas as interfaces de fronteira principais.
  - Fluxo de usuário/grupo inferência de geração -interface de acesso do usuário/grupo.
- Saída vs. Entrada monitoramento:
  - Matriz de tráfego inferência – ingresso OU saída.
  - Fluxo de usuário/grupo inferência de geração - ambas direcoes.

	A	B					
A		?	?	?	?	?	?
B	?		?	?	?	?	?
C	?	?		?	?	?	?
D	?	?	?		?	?	?
E	?	?	?	?		?	?
F	?	?	?	?	?		?
G	?	?	?	?	?	?	

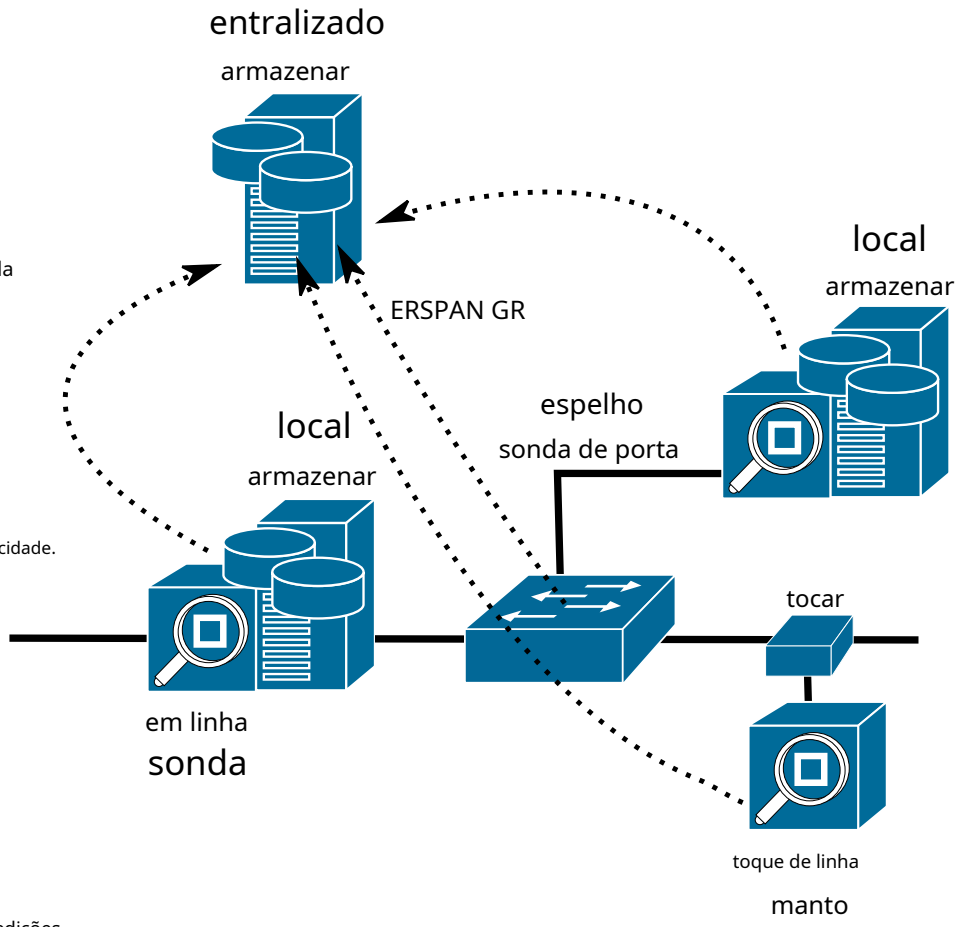


IPFIX (v10) e NetFlow flexível

- IPFIX é muito semelhante ao NetFlow v9
  - Usa a versão 10 em um cabeçalho semelhante.
  - Também possui modelos e registros de dados.
  - Também possui modelos de opções e registros de dados de opções.
- A IPFIX fez provisões para o NetFlow v9 e adicionou suporte para ele.
  - O IPFIX lista uma visão geral dos “identificadores de elementos de informação” que são compatíveis com os “tipos de campo” usados pelo NetFlow v9.
- O IPFIX possui mais tipos de arquivos do que os definidos para NetFlow v9.
  - Também permite que um ID de fornecedor seja especificado que um fornecedor pode usar para exportar informações proprietárias/genéricas.
- IPFIX permite campos de comprimento variável.
  - Útil para exportar strings de tamanho variável (por exemplo, URLs).
- A extensão NetFlow v9 “Flexible NetFlow” pretende ser tão flexível quanto o IPFIX.

Sondagem Passiva de Rede

- Usuário para:
  - Inferência de dados específica e detalhada,
  - Inferir dinâmicas de pequena e média escala de tempo.
- Tipos de sonda
  - Trocar porta de espelho,
  - Em linha,
  - Toque de rede.
  - Túnel ERSPAN GRE do switch.
    - ERSPAN: Analisador de porta comutada remota encapsulada
- Filtrando/amostrado por
  - Usuário/endereço do terminal/VLAN/porta de acesso,
  - Endereço de grupo/VLAN/porta de acesso,
  - Protocolos (UDP/TCP),
  - Protocolos de camada superior,
    - Difícil de identificar devido à criptografia e restrições legais/de privacidade.
  - Número/intervalo da porta UDP/TCP.
- Processamento de dados
  - Contagem de pacotes/bytes,
  - Contagem de fluxo,
  - Endereços IP e distribuição de portas,
  - Estatísticas e distribuição de aplicativos/serviços.
- Armazenamento e processamento local versus centralizado.
  - O upload de dados para um ponto centralizado não deve ter impacto nas medições.
  - O armazenamento/processamento local requer análises com mais recursos.



Sistemas de gerenciamento de logs (LMS)

- Sistema de software que agrega e armazena arquivos de log de diversas fontes e sistemas de rede.
- Permite que as organizações centralizem todos os seus dados de log de vários sistemas.
- Permite que os Logs sejam visualizados e correlacionados.
- Principais finalidades:
  - Detectar e responder a Indicadores de Comprometimento (IoC);
  - Realizar análise de dados forenses;
  - Realize investigações sobre eventos de rede e possíveis ataques.

Informações e eventos de segurança Gestão (SIEM)

- Incorpora três tipos de ferramentas de segurança em um único aplicativo:
  - Gerenciamento de Eventos de Segurança (SEM)
    - Muito semelhante ao LMS.
    - Agrega arquivos de log de vários sistemas, mas eles são mais voltados para as necessidades dos analistas de segurança de TI do que dos administradores de sistema.
  - Gerenciamento de informações de segurança (SIM)
    - Ferramentas de software usadas para identificar, coletar e analisar dados de logs de eventos.
    - Inclui recursos automatizados e alertas que podem ser acionados quando condições predeterminadas são satisfeitas e podem indicar que a rede está comprometida.
    - Ajude os analistas de segurança a automatizar o processo de resposta a incidentes e gerar relatórios mais precisos sobre a posição/passado de segurança da organização.
  - Correlação de Eventos de Segurança (SEC)
    - Software usado para processar e pesquisar grandes quantidades de logs de eventos e descobrir correlações e conexões entre eventos que possam indicar um problema de segurança.

LMS x SIEM

- As ferramentas LMS estão mais focadas em:
  - Coleta de dados de log, retenção eficiente de dados, indexação de log e funções de pesquisa e relatórios.
- As ferramentas SIEM estão mais focadas em:
  - Alertas de detecção de ameaças, correlação de eventos e dashboard (monitoramento em tempo real com visibilidade de eventos personalizados).
- A evolução dos LMS tradicionais, projetados principalmente para suporte à administração de sistemas, tornou-os funcionalmente muito mais próximos das ferramentas SIEM desenvolvidas do zero como ferramenta de segurança.

Eventos SIEM (exemplos)

- Detecção de força bruta
  - Erros 404 excessivos (log do servidor HTTP) de um cliente não autenticado (log do banco de dados). Falhas
  - excessivas de login (serviços ou logs de banco de dados) em um ou vários serviços.
    - De um endereço IP específico (ou conjunto de endereços IP).
    - De regiões geográficas “estranhas” ou AS.
  - Credenciais não correspondentes
    - De máquinas internas com credenciais de usuário não correspondentes (logs RADIUS/LDAP).
- Viagem impossível
  - Vários logins do mesmo usuário em diferentes dispositivos/locais.
  - Logins consecutivos do mesmo usuário de regiões geográficas distantes em um pequeno intervalo de tempo. O uso de VPN pode acionar esse alarme.
- Transferência de dados anômala
  - Análise por origem individual (IP ou grupo de dispositivos) e/ou destino e/ou por protocolo/porta utilizado.
  - Transferência de dados excessiva/diferente não compatível com observações anteriores
    - Uso de protocolos e portas;
      - Geralmente as regras de firewall resolvem isso!
    - Quantidades de download/upload, número de conexões, proporção upload/download, proporção DNS/não-DNS, etc...; Nunca
    - entrei em contato com dispositivos: servidores externos (IP/ASN ou país desconhecido) ou dispositivos internos; Hora absoluta
    - do dia/semana/mês.
    - Atividade em tempo relativo: média ou desvio padrão dos intervalos entre atividades/fluxos/solicitações/etc...
  - Deve ser usado para detectar exfiltração (ou propagação dentro da rede) e C&C e canais de dados ilícitos.
- Ataque DDoS
  - Tentativas excessivas de conexão de dispositivos/endereços/regiões “nunca vistos”.
    - Detecção ideal na fase inicial do ataque.
  - Tentativas não excessivas, mas comportamento não conforme (comportamento temporal, sequência de solicitações, etc...)
    - Mais difícil de definir.
- A integridade dos arquivos/configurações falha
  - Falha na soma de verificação do arquivo de configuração de dispositivo/serviço específico, não justificável pelas ações observadas. Falha
  - genérica na soma de verificação do arquivo, não justificável pelas ações observadas.
- Etc...?

Centro de Operações de Segurança (SOC)

- Competências de um SOC em uma organização:
  - Prevenção e detecção de ataques
    - Monitore rede e serviços (com SIEM)
    - Detectar vulnerabilidades (com ferramentas de verificação de
    - vulnerabilidades) Detectar atividades maliciosas (com SIEM)
    - Detecte comportamentos anômalos (com SIEM)
      - pode não ser malicioso!
  - Investigação
    - Analisar a atividade suspeita para determinar/caracterizar a ameaça
    - Avaliar a profundidade da penetração da ameaça na rede/sistemas
  - Resposta
    - Implemente contra-medidas com base em manuais conhecidos
    - Implemente medidas de emergência quando a ameaça não corresponder a um manual de resposta conhecido
  - forense
    - Feito após um ataque
    - Reunir evidências para fins judiciais
    - Reúna dados adicionais para melhorar o fut(NOC), a aquisição de dados e a mitigação de ameaças (NDR por NOC).ure prevenção/detecção/resposta
- Hoje em dia comumente operado independentemente do Network Operation Center (NOC).
- Deve ser integrado ao NOC.
  - Para segregação e resiliência de redes/serviços, aquisição de dados e mitigação de ameaças.