

# ***Monitoramento de Redes***

Prof. Thiago Nelson

# ***Analísadores de Protocolos***

- Ferramenta de gerenciamento de falhas e desempenho de uma rede.
- Captura o tráfego gerado na rede;
- Decodifica os protocolos nos pacotes capturados;
- Provê estatísticas sobre, por exemplo:
  - Carga oferecida na rede;
  - Taxa de erros;
  - Tempo de resposta.

# ***Analizadores de Protocolos***

- **Exemplos:**
  - ***Ethereal (Open Source);***
  - ***Sniffer Network Analyzer (Network Associates)***
  - ***NetXRay (Network Associates);***
  - ***EtherPeek (Wild Packets);***

# ***Analísadores de Protocolos***

- **Lembrar que um analisador de protocolos pode ser uma “arma” na mão de pessoas mal intencionadas!**
- **Com recursos de armazenamento e filtragem de pacotes obtidos de uma interface de rede colocada de modo promíscuo é possível obter logins e senhas de usuários.**

# Ferramentas de Monitoramento

- ***MIB (Management Information Base) RMON (Remote Monitoring) desenvolvido pela IETF (Internet Engineering Task Force)***
  - Obtém estatísticas sobre parâmetros da camada de enlace de dados e da camada física, por exemplo:
    - Tamanho das estruturas;
    - Colisões de Ethernet;
    - Taxa de erros Token Ring;
    - Taxa de pacotes de difusão

# Ferramentas de Monitoramento

- **NAGIOS**
- *Open Source;*
- Monitora quaisquer equipamentos de rede:
  - Verifica se o equipamento está ou não ligado;
  - Monitorar a disponibilidade dos serviços de rede que estão sendo executados;
  - Monitora os recursos (carga de processador, uso de memória e disco, processos em execução);
- Envio de notificação (via e-mail, SMS, etc.) quando um problema ocorrer ou quando o mesmo estiver solucionado;
- Interface web para visualizar estado atual da rede, histórico de problemas, arquivos de log, etc.

# Ferramentas de Monitoramento

- ***CiscoWorks***
  - Conjunto de aplicativos de *software para gerenciar* redes com base no protocolo SNMP (*Simple Network Management Protocol*).
  - Permite o monitoramento de dispositivos, a manutenção da configuração e a solução de problemas de dispositivos Cisco.

# Ferramentas de Monitoramento

- **MRTG (*Multi Router Traffic Grapher*)**
  - Ferramenta para monitoramento da carga de tráfego da rede.
  - Gera páginas HTML contendo imagens que representam graficamente e em tempo real, o tráfego da rede.
  - MRTG é baseado em C e Perl;
  - Muitos sites utilizam o MRTG para monitorar compromissos de QoS e fazer cobranças dos clientes com base no uso da rede.

# Ferramentas de Monitoramento

- Grupos de pesquisas e debates sobre ferramentas de medição de redes:
  - CAIDA (*Cooperative Association for Internet Data Analysis*)
    - <http://www.caida.org>
  - IPPM (*Internet Protocol Performance Metrics*) da IETF
    - <http://www.advanced.org/IPPM/>
  - ISMA (*Internet Statistics Measurement and Analysis*) Workshop
    - <http://www.caida.org/outreach/isma/>

# Referências

- **Ethereal: A Network Protocol Analyzer.**
  - Disponível em: <http://www.ethereal.com>
- **MRTG: The Multi Router Traffic Grapher.**
  - Disponível em: <http://mrtg.hdl.com>
- **Nagios.**
  - Disponível em: <http://www.nagios.org>