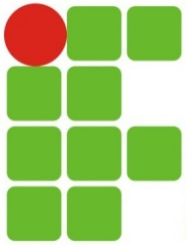


INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Gerência de Redes de Computadores
Introdução

Prof. Alex Furtunato

alex.furtunato@academico.ifrn.edu.br

Administrar x Gerenciar

- Termos sinônimos nos dicionários:
  - Administrar
    - Ajudar, auxiliar, gerir, governar, …
  - Gerenciar
    - Gerir, ter gerência sobre, administrar, dirigir, gerenciar, regular …
- Em Redes de computadores, porém, tem significados diferentes

Administrar Redes

- Disponibilizar serviços e aplicações para a infra-estrutura de rede:
  - Serviços de diretório
  - Administração de contas de usuários/senhas
  - Sistemas de arquivos
  - Cotas de discos
  - Serviços de intranet (NFS, Smb, Impressão, DHCP, Terminal, etc)
  - Serviços de Internet (DNS, WWW, FTP, email, etc)

Gerenciar redes

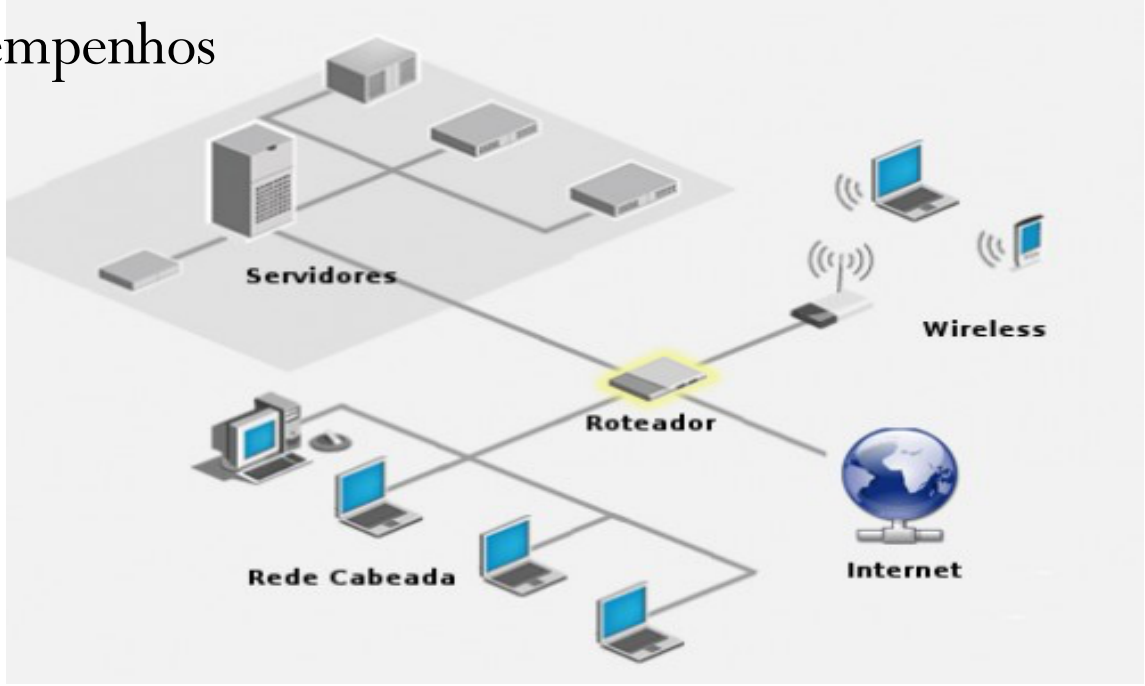
- Monitorar e acompanhar o funcionamento da rede de computadores
  - Avaliando o seu desempenho
  - Encontrando indicadores de uso
  - Identificando falhas
  - Identificando tentativas de invasão
  - Identificando perdas de conexões
  - Garantindo a disponibilidade dos serviços

Contexto atual

- Crescimento das redes, do número de equipamentos e da diversidade de tecnologias
- Novos dispositivos de rede
  - BYOD – Bring Your Own Device (Traga seu Prórpio Dispositivo) - Video
- A rede como área estratégica dentro das corporações
- Aumento exponencial do número de fabricantes
- Diversidade de sistemas proprietários de gerenciamento
- Aumento do número de serviços disponibilizados na rede
- Sofisticação de funcionalidades dos equipamentos e acessórios

Rede de computadores

- Para um bom gerenciamento de uma rede, é preciso CONHECÊ-LA:
  - Quais equipamentos compõem a rede
  - Como é a interconexão entre eles
  - Quais os seus desempenhos
  - MÉTRICAS

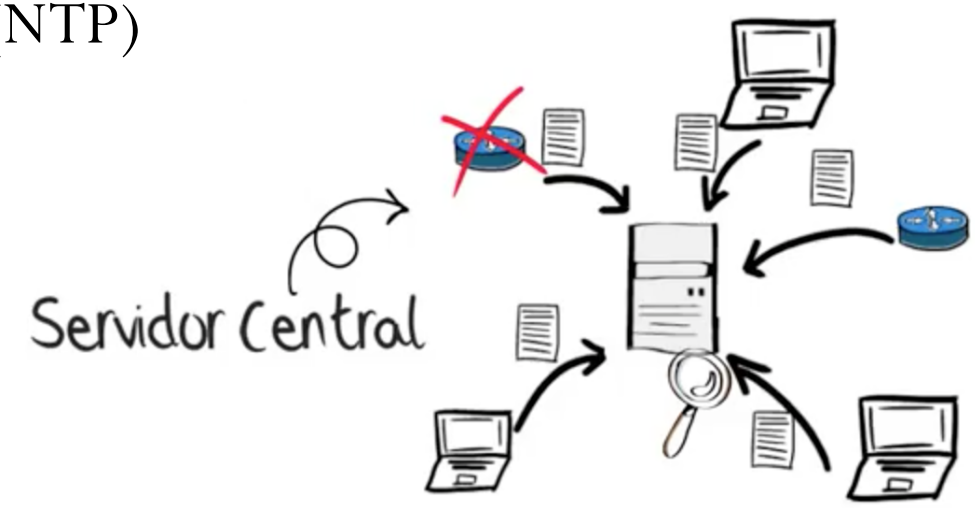


Organização da rede

- Diagrama e documentos da rede
- Inventário dos equipamentos
- Backup de configurações
- Registros de eventos

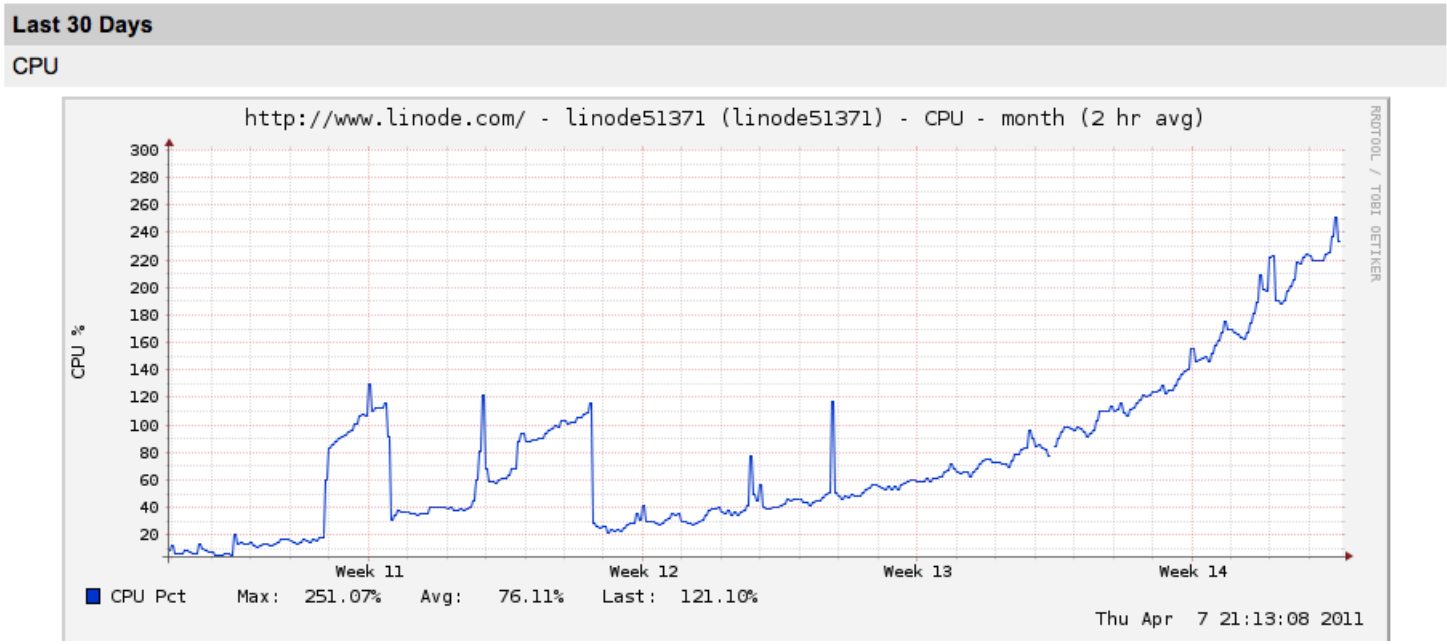
Registro de eventos

- Logs de servidores e equipamentos
  - Históricos de acessos
  - Execução de programas e scrips
  - Eventos de erros ou “warnings”
  - Logs centralizados
    - Correlação de eventos (SIEM)
  - Sincronismos de tempo (NTP)
    - Coerência de logs



Reconhecer comportamento

- Experiência com a rede ou,
- Métricas com “BASELINE”
  - Velocidade
  - Throughput (Taxa de transferência)
  - Disponibilidade



Gerenciamento de redes

- Está associado ao controle de atividades e ao monitoramento do uso de recursos de rede
- Atividades comuns:
  - Obter informações da rede;
  - Registrar a ocorrência de eventos;
  - Estabelecer critérios para o disparo de alarmes;
  - Detectar e diagnosticar a ocorrência de falhas;
  - Conhecer e controlar alterações em equipamentos;
  - Acompanhar o desempenho da rede e serviços;
  - Garantir a segurança;
  - Contabilizar recursos.

Por que gerenciar?

- Devido a importância das redes de computadores em relação aos negócios das instituições e a seus clientes
- Devido ao porte e a complexidade das mesmas
- As redes de computadores atuais são extremamente heterogêneas
- Sem um controle efetivo, os recursos não proporcionam o retorno que a instituição necessita
- Garantir a qualidade esperada da infra-estrutura de rede
- Identificar padrões e tendências de uso
- Planejar o crescimento da rede
- Identificar e resolver problemas o mais breve possível

O que gerenciar?

- São várias as possibilidades de equipamentos ou serviços passíveis de gerenciamento:
  - Ativos de rede;
  - Aplicações e serviços de rede;
  - Bancos de dados;
  - Dispositivos de armazenamentos;
  - Dispositivos de Potência e monitoração de ambientes;
  - Acessórios diversos;

- Que tipos de equipamentos podemos gerenciar na rede de uma empresa?
  - Switch, Servidores, Ar-condicionado, No-break, Estações de trabalho, Rádios Wifi, Câmeras IP, Telefones IP, etc

Problemas mais comuns

- Rede lenta
- Rede indisponível
- Recursos mal utilizados
- Sobrecarga do uso de recursos
- Problemas de segurança

- Consequência da falta de gerenciamento
  - Perda de tempo para resolução de problemas
  - Impossibilidade de solução do problema

Áreas funcionais

- A international Organization of Standard (ISO) criou um modelo de gerenciamento com cinco áreas funcionais:
  - Gerenciamento de falhas (**F**ault)
  - Gerenciamento de configuração (**C**onfiguration)
  - Gerenciamento de contabilização (**A**ccount)
  - Gerenciamento de desempenho (**P**erformance)
  - Gerenciamento de segurança (**S**ecurity)

- Modelo também conhecido como **FCAPS**

Gerência de falhas

- Assegurar a operação contínua;
- Detectar, isolar o problema;
- Registrar as ocorrências de falhas;
- Executar testes de diagnóstico;
- Isolar o componente que falhou;
- Atuar de modo proativo ou reativo, reparando ou trocando o componente que falhou;

- Ex:
  - Monitorar enlaces, monitorar serviços, etc.

Gerência de configuração

- Coletar informações sobre a topologia da rede;
- Monitorar mudanças na estrutura física e lógica;
- Alterar a configuração dos elementos gerenciados;
- Manter equipamentos atualizados;

- Ex:
  - Atualização de firmwares, documentar mudanças de configuração, etc.

Gerência de contabilização

- Controlar o uso dos recursos;
- Aplicar tarifas aos recursos (discos, banda, telecomunicações, email, etc);
- Viabilizar e identificar os custos;
- Manter limites de uso;
- Efetuar a melhor distribuição dos recursos;

- Ex:
  - Números de acessos, número de impressões, banda de acesso, etc.

Gerência de desempenho

- Mensurar, analisar e controlar o desempenho dos componentes da rede;
- Monitorar a operação diária da rede;
- Localizar pontos críticos;
- Registrar dados de operações;

- Ex:
  - Medir a taxa de utilização. Qual a capacidade? O tempo de resposta é considerável? Precisa substituir equipamento?

Gerência de segurança

- Cuidar dos mecanismos e procedimentos de segurança;
- Garantir a aplicação da política de segurança;
- Controlar o acesso a rede e as informações;
- Mantem registros de eventos relacionados a segurança;

- Ex:
  - Gerar relatórios de uso de recursos, Analisar logs dos sistemas, checar direitos de acessos, etc.

Gerente de Rede

- Atividade principal:
  - Prevenir e Solucionar os problemas apresentados na rede
    - Detectá-los
    - Localizá-los
    - Solucioná-los
- Normalmente fala-se de "Equipe de Gerência de Rede"
  - Central de Serviço – Níveis, SLA
  - Técnicos
  - Gerente de equipe

Gerência de Rede versus Medicina

- No dicionário Medicina é definida como: “Arte e ciênca de prevenir e curar as doenças”
- Essa definição poderia ser reescrita para o Gerente de Rede:
  - “Arte e ciência de prevenir e solucionar problemas de rede”
- Baseado nessa analogia poderemos comparar algumas similaridades

Gerência de Rede versus Medicina

Medicina	Gerência de Redes
Algumas "doenças"podem ser previnidas e outras não Ex: AIDS, Doenças hereditaria	Alguns "problemas de rede"podem ser previnidos, e outros não Ex: Configuração errada, Queima de equipamento
O médico através de perguntas busca os "sintomas"	O Gerente busca os sintomas de diversas formas ("A rede não fala")
Através de instrumentação adequada são feitos examens para buscar "sinais" de doença	O gerente através de ferramentas busca informações e as interpreta na busca por "sinais" do problema. (Em geral, usuários não tem como detectar sinais)

Gerência de Rede versus Medicina

Medicina	Gerência de Redes
Doenças podem apresentar sinais típicos. Esses sinais são chamado patognomônicos	Na gerência de redes, opdem haver sinais desse tipo que podemos chamar de "sinais diferenciais". Nesse caso o problema foi descoberto. Ex: Bloqueio de rede
Se sintomas e sinais coletados, por si só, não confirmam uma doença, faz-se "Testes confirmatórios" adicionais para confirmar ou negar suspeitas	Alguns problemas podem ter mais de uma causa. Nesse caso, faz-se "Testes confirmatórios" para validar cada possível causa. Ex: Ponto de rede ou Placa de rede, ou ...
Muitas doenças podem ser descobertas antes de qualquer sintoma surgir. Ex: Cancer de mama	Problemas de rede podem ser detectados antes de usuários perceberem. Ou podem ser antecipados antes de surgirem. Ex: Monitoramento ativo de componentes (Discos de Storage)

Exemplos de Problemas

Camada	Descrição
Camada Física	- Cabo rompido - Conector Defeituoso - Placa de rede com defeito - Interferência
Camada de Enlace	- Interface desabilitada - Problemas com tabela ARP
Camada de Rede	- Rotas mal configuradas - VLANS não configuradas - Servidor DHCP mal configurado
Camada de Aplicação	- DNS não habilitado - Servidor Web mal configurado - Servidor de email com relay aberto

Metodologia Geral de Detecção, Diagnóstico e Solução de Problemas

1. Detecção do Problema
   - Usuários reportam sintomas
   - Operador percebe equipamentos e/ou serviços com problemas
2. Coletar informações
   - Quem está send afetado? Apenas um usuário ou todos? Numa mesma subrede?
   - Quando o problema iniciou? Ocorre apenas em certos horários?
   - Afeta apenas alguns serviços?
   - Alguma mensagem de erro?

Metodologia Geral de Detecção, Diagnóstico e Solução de Problemas

3. Recorrente? Houve mudança de rede?
   - Se recorrente, pode ter a mesma causa detectada anteriormente
   - Houve mudança recente na rede? Provavelmente a mudança causou o problema
4. Desenvolver hipóteses
   - Conhecimento técnico e experiência
   - Brain storm
5. Testar as hipóteses
6. Solucionar problema
7. Documentar a solução

Exemplo de sintoma

Sintoma: Usuário reclma de falta de conectividade
Cabo rompido ou danificado
Conector defeituoso ou mal instalado
Equipamento de interconexão defeituoso
Placa de rede ou porta de equipamento de interconexão defeituosos
Interface desabilitada
Saturação de recursos devido a excesso de broadcast
Validade da cache ARP inadequada
Rotas mal configuradas (em roteadores)
VLAN incorreta
Problema com spanning three
Equipamento do usuário
O próprio usuário

Histórico de Gerência de Redes

- Até o final da década de 70
  - Não existia protocolo de gerenciamento de rede
  - Utilizava-se apenas ICMP (Internet Control Message Protocol)
  - Utilitário PING (Packet Internet Groper)
- No final da década de 80
  - Internet cresceu exponencialmente
  - Buscaram-se soluções para melhorar o gerenciamento
    - SGMP – Monitoração de roteadores
    - HEMS – High Level Monitoring Protocol
    - CMOT – CMIP (Common Management Information Protocol) over TCP/IP
    - SNMP – Como expansão do SGMP
  - Em 1988, IAB (Internet Activities Board) aprova o SNMP como solução de curto prazo e o CMOT como uma solução a longo prazo

Histórico de Gerência de Redes

- Após padronização, o SNMP passou a ser bem aceito
  - Todos os fabricantes o adotaram
  - SNMP vira padrão de fato
  - CMOT foi abandonado
- SNMP
  - 1989 – SNMPv1
  - 1991 – RMON
  - 1995 – SNMPv2
  - 1997 – RMON2
  - 1998 – SNMPv3

Padrões de gerenciamento

- OSI/CMIP (Open System Interconnection/Common Management Information Protocol)
- SNMP/Internet (Simple Network Management Protocol)
- TMN (Telecommunications Management Network)

OSI/CMIP

- Padrão ISO (*International Organization for Standardization*)
- Classificou a gerência em 5 áreas funcionais
- Gerenciamento de redes LAN/WAN
- Complexidade e lentidão do processo de padronização impediu a sua adoção

SNMP/Internet

- Padrão IETF (Internet Engineering Task Force)
- Incialmente para gerenciamento de componentes Internet
- Atualmente utilizado em sistemas de telecomunicações e WAN
- Fácil de implementar
- Atualmente existem 3 versões:
  - SNMPv1
  - SNMPv2
  - SNMPv3

TMN

- Padrão ITU-T (International Telecommunication Union)
- Gerenciamento de redes de telecomunicações

Network Operation Center (NOC)

- Consiste em um conjunto de atividades realizadas para manter dinamicamente o nível de serviço em uma rede ou conjunto de redes. Estas atividades asseguram alta disponibilidade de recursos pelo rápido reconhecimento de problemas, disparando funções de controle quando for necessário

Network Operation Center (NOC)

Network Operation Center (NOC)