Segurança Cibernética

Princípios de Segurança Cibernética I

Prof. Dr. Daniel Caetano

2021 - 2

Compreendendo o problema

- **Situação:** Quando se pensa em segurança da informação, se pensa em vultosos investimentos em equipamentos e tecnologia.

Mentimeter

Do que estamos protegendo a informação?

Compreendendo o problema

- **Situação:** A informação está armazenada nos "storages", equipamentos que buscamos proteger.

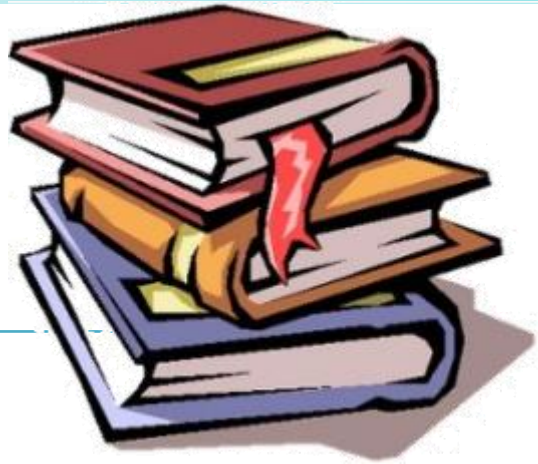
Mentimeter

Mas como chegam onde são necessárias?

Objetivos

- Conhecer as informações que precisamos proteger
- Tomar contato com o nosso contexto de atuação
- Alguns mecanismos de recuperação
- Tomar contato básico com o funcionamento do tráfego de rede

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	https://www.caetano.eng.br/aulas/2021b/ara0076.php (Segurança Cibernética – Aula 2)
Minha Biblioteca	• Segurança de Computadores e Teste de Invasão (ISBN: 978-0-8400-2093-2), págs 11 a 101. • Segurança de Computadores: Princípios e Práticas (ISBN: 978-85-352-6449-4), págs 10 a 19; • Redes de computadores: uma abordagem top-down (978-85-8055-169-3), págs 34 a 42.
Material Adicional	1) 5 ferramentas de segurança para proteger sua rede! - Dispoinível em: https://youtu.be/CInn1mpc67M

Antes de Mais nada...

- **Consulte o material da 1ª Aula!**
- **Otimize seus estudos**
  - Se preparar para conteúdo da semana seguinte!
- **Atividades e Desafios Semanais**
  - No site e mural da disciplina: https://www.caetano.eng.br/aulas/2021b/ara0076.php
- **Será controlada a presença**
  - Chamada ocorrerá sempre nos 15 minutos finais
- **Contato**

Professor	E-mail
Daniel Caetano	prof@caetano.eng.br

Visão Geral:

O que, de quê e como proteger?

O que envolve a segurança?

- Elementos
  - Hardware, software, dado, instalações/rede
- Terminologia
  - Ameaça, vulnerabilidade, ataque/incidente
  - Risco, impacto/desastre
  - Contramedidas, política e plano de segurança

Política x Plano de Segurança

- Política de Segurança da Informação
  - *Information Security Policy*
  - Planejamento/gerenciamento de segurança
    - Preocupação ampla com segurança
    - Física, lógica, contingência etc.
- Segurança de TI (ou *Cybersecurity Plan*)
  - Parte da PSI que trata de:
    - Monitoramento de login
    - Proteção dos servidores (uso de recursos e dados)
    - Proteção do tráfego de dados (criptografia)
    - Gerenciamento de servidores (remoto)
    - Realização de backups

O que precisa ser protegido?

- Dados gerais que são parte da operação
- Dados estratégicos
- Dados associados às leis gerais
  - Lei Geral de Proteção de Dados
  - Marco Civil da Internet...

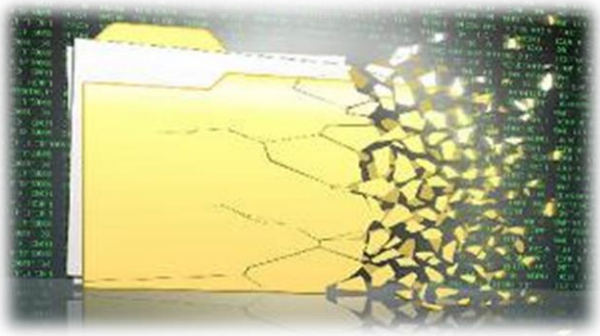
- Dados associados às leis específicas
  - Tributária, sanitária...
- Foco: evitar exposição e perda de dados
  - Adicional: evitar uso abusivo dos dados

Classificação das Informações

- Cuidados dependem da importância
  - Públicas
    - Publicação ou perda não acarreta prejuízos
  - Internas
    - Publicação ou perda não tem consequências sérias
  - Confidenciais
    - Publicação ou perda pode acarretar problemas significativos (perdas financeiras, de clientes ou de credibilidade)
  - Secretas
    - Publicação ou perda pode ser desastrosa

Qual o foco dos ataques/invasões?

- Dados
  - Roubar, sequestrar, destruir...
- Só dados?
  - Não!
- Uso de poder computacional e banda de rede
  - Ataques a outros computadores
  - Botnets para usos ilegais
  - Processar criptomoedas...

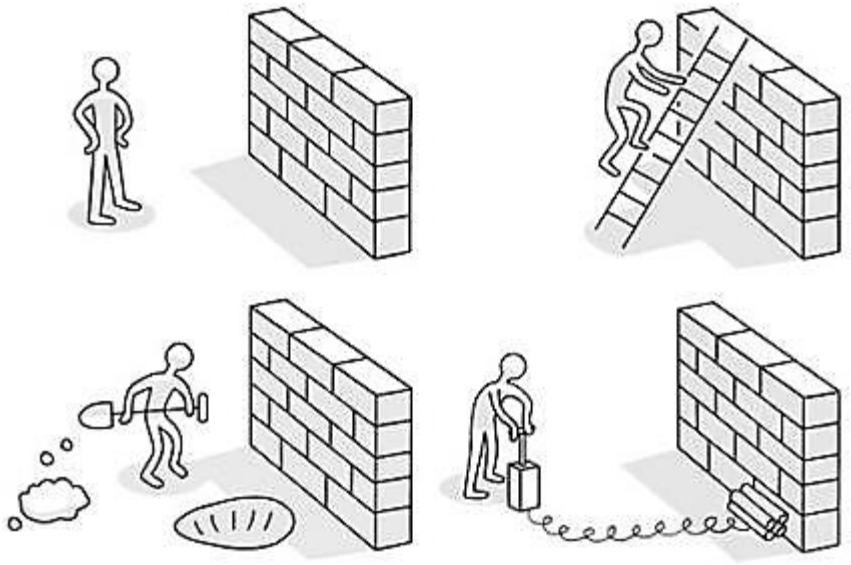


Situações indesejáveis

- Revelação não autorizada
  - Quebra de confidencialidade
  - Exposição, interceptação, inferência, intrusão;
- Fraude
  - Quebra de integridade de dados ou sistema
  - Personificação, falsificação, retratação/repúdio;
- Disrupção
  - Quebra da disponibilidade ou integridade (D/S)
  - Incapacitação, corrupção, obstrução;
- Usurpação
  - Quebra da integridade do sistema
  - Apropriação indevida, utilização indevida.

Quem faz a proteção?

- Equipe de segurança
  - Interna: funcionários experientes contratados
  - Hackers éticos: identificar vulnerabilidades
    - Descobrir problemas antes que um antiético o faça!
  - Em todo o caso, devem considerar:
    - As leis
    - As regras da empresa



Desviando do perigo

- Evitar a exploração de vulnerabilidades
  - Situação x Exemplo de contramedida:
    - Indisponibilidade de comunicação
      - Redundância de sites
    - Perdas por desastres diversos
      - Cópias de segurança (*backup*)
    - Exploração de vulnerabilidades
      - Mitigar vulnerabilidades
        - » Engenharia Social
        - » Farejadores (sniffers)
        - » Falhas no TCP/IP
        - » ...

VISÃO GERAL:

REDUNDÂNCIA E CÓPIAS DE SEGURANÇA

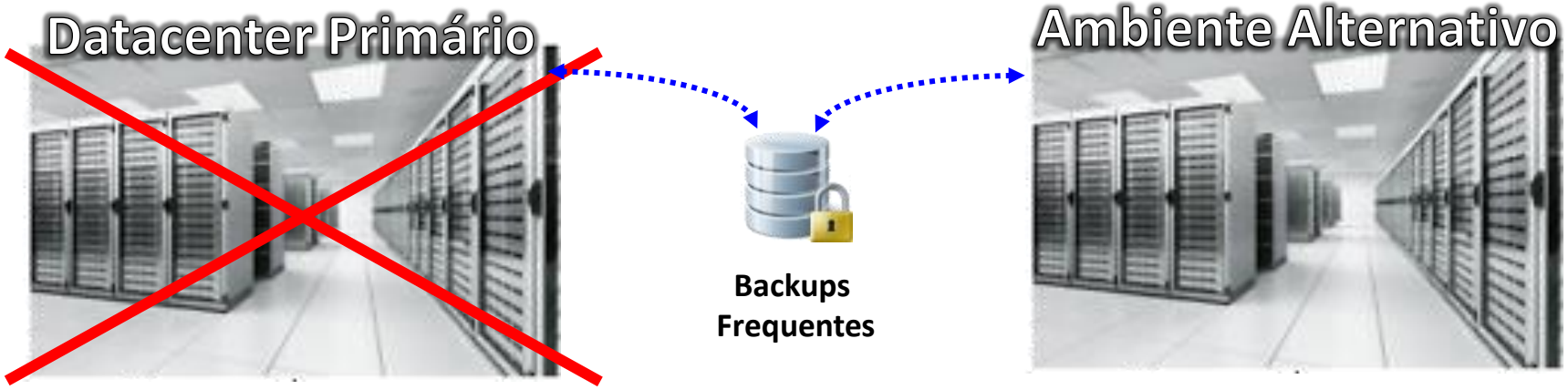
Redundância

- O que é?
- Básica: nos próprios equipamentos
  - *Servidores* redundantes e paralelos
  - *Storage*, equipamento de *backup* etc.
- E num desastre maior...?
  - O que fazer?

- Primeira ação: continuidade de operação
  - Até reconstrução e restauro dos backups...

Ambientes Alternativos

- Ajuda se existir um ambiente “espelho”
  - Ambientes de operação alternativos
- Três tipos
  - Cold Site
  - Warm Site
  - Hot Site



Ambientes Alternativos

Cold Site

- Pouco ou nenhum equipamento
- Se conectividade de rede significativa
- Ativação manual
- Sem sincronia de dados
- Alta chance de perda de dados
- Custo baixo

Recuperação em **semanas/dias**

Warm Site

- Equipamento parcialmente redundante
- Conectividade de rede ativa
- Ativação automática em caso de falha
- Sincronia de dados diária ou semanal
- Pequena perda de dados
- Custo mediano

Recuperação em **dias/horas**

Hot Site

- Equipamento totalmente redundante
- Conectividade de rede ativa de alta performance
- Sempre ativo
- Sincronia em tempo real (ou quase)
- Nenhuma perda de dados
- Custo elevado

Recuperação em **horas/minutos**

Todos: Complexidades + Custos

Backups

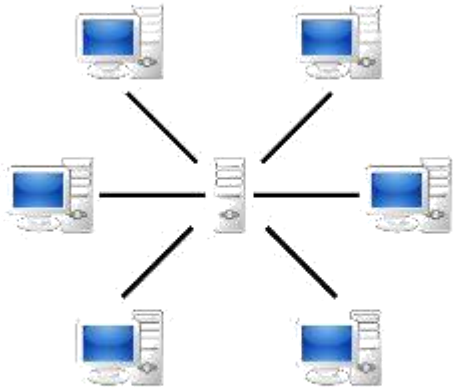
- Frequência: não prejudicar os negócios
  - Limitações: espaço, tempo e desempenho
- Abrangência: o que for necessário (dados + cfg)
  - Sistema: completo ou completo + diferencial
- Mídia: conveniência e segurança (storage, fita)
  - Ameaças, tempo de vida e quantidade de dados
  - Tempo e frequência de recuperação
  - Custo!
- Localidade: local ou nuvem?
  - Evitar desastre duplo, custo, banda...

Parênteses Estratégico:

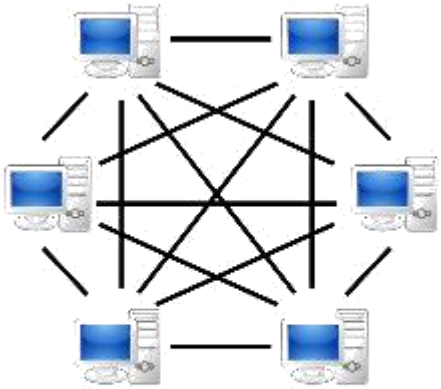
O Tráfego nas Redes e Internet

Contexto do tráfego de rede

- Comunicação entre máquinas e serviços
  - Paradigmas:
    - Cliente-Servidor
    - Peer 2 Peer
    - Misto.
- Comunicação usual
  - Sockets
  - Protocolos: UDP/TCP
- Funcionamento e origens...
  - Explicam muitas das limitações

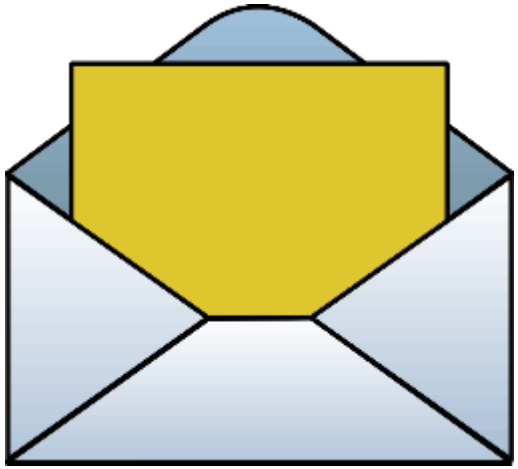


Server-based



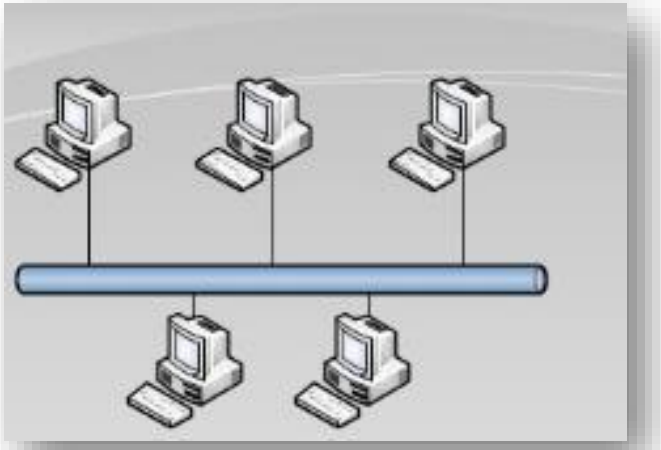
P2P-network

Como funciona o correio?



Origens

- Redes locais x Inter-net



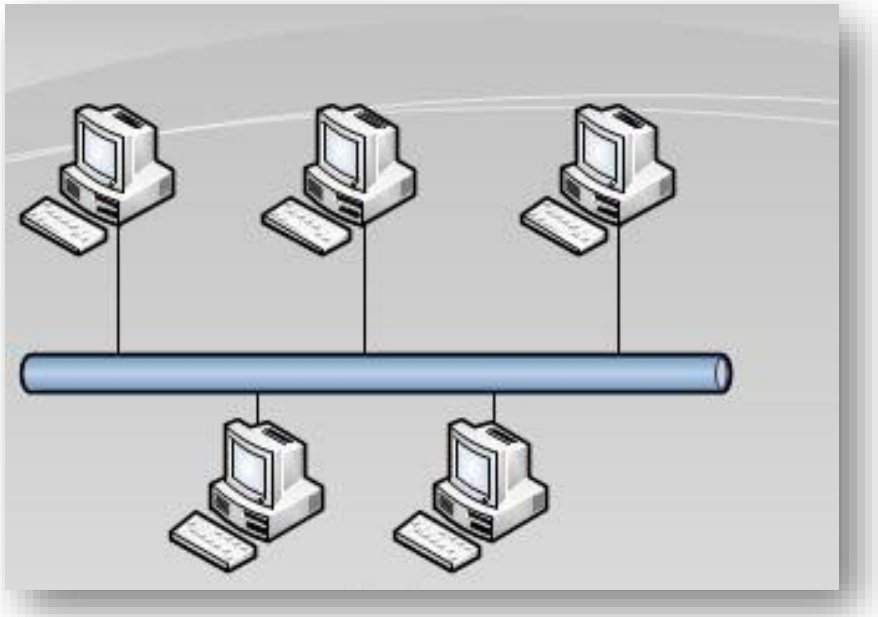
Rede Local: vila

Internet: cidade

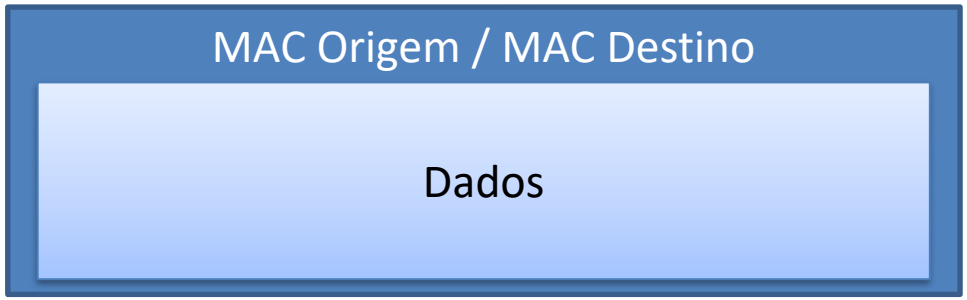
- Diferença importante:
  - Organização do tráfego de dados

Rede Local: Comunicação Direta

- Pacote com dado em contexto local

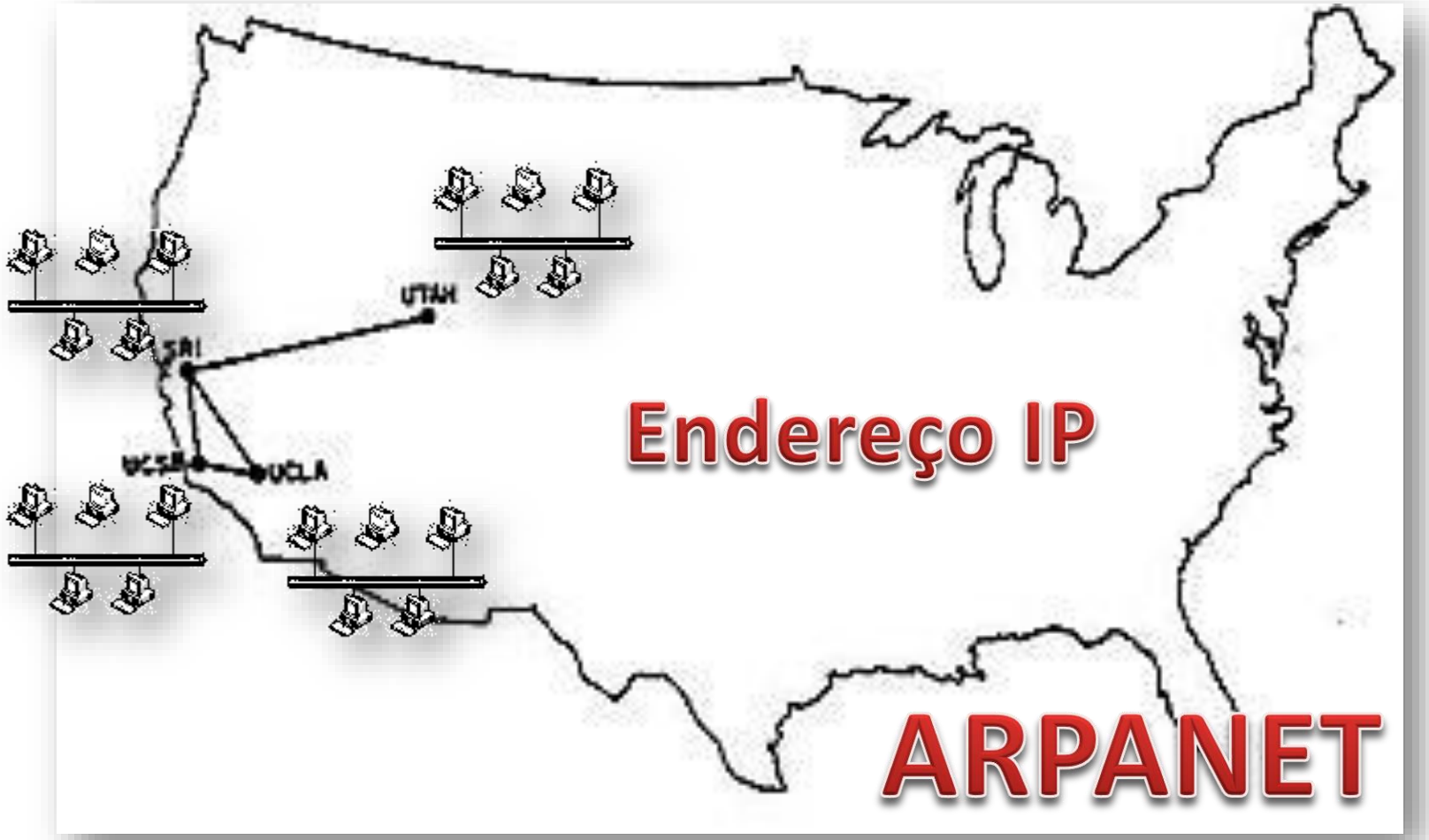


Endereço MAC



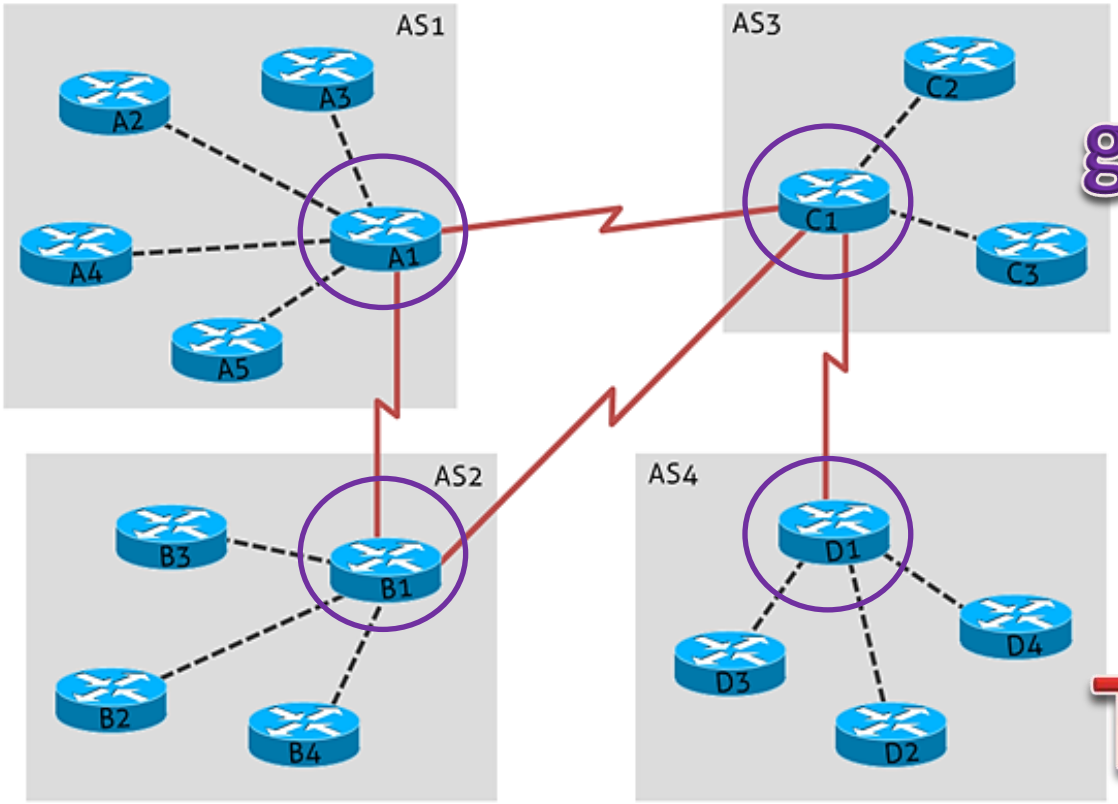
Rede: vila
MAC: nome da pessoa

Internet: interligando redes



Internet: Comunicação Hierárquica

Rede: cidade
MAC: nome
IP: endereço



gateways

arp -a

IP

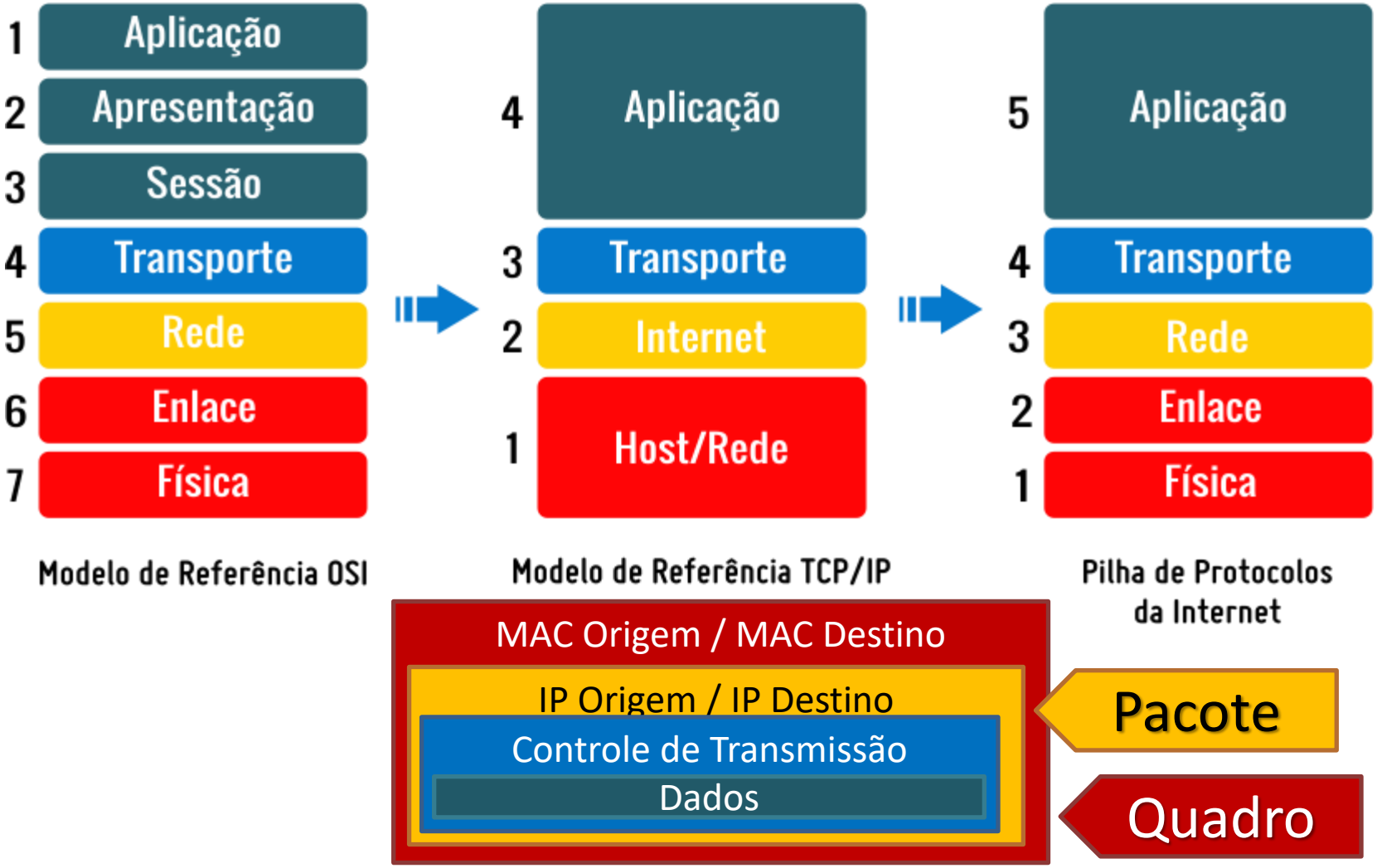
TCP/IP

MAC Origem / MAC Destino
IP Origem / IP Destino
Dados

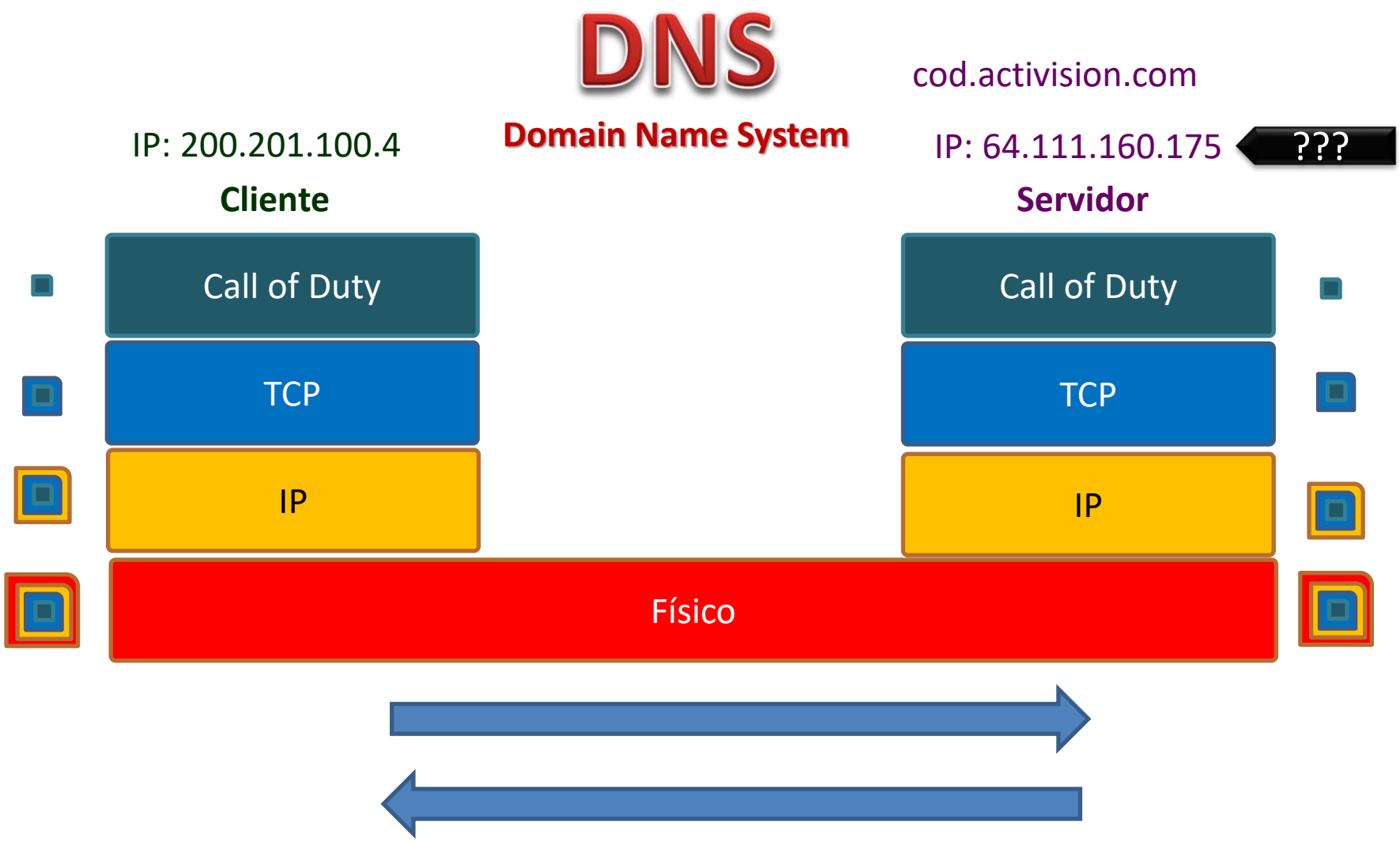
MAC Origem / MAC Destino
IP Origem / IP Destino
Controle de Transmissão
Dados

Protocolos

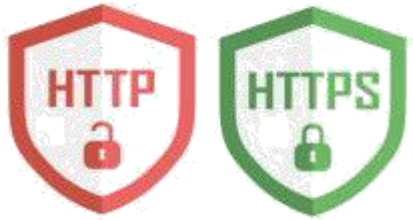
- Comunicação padronizada



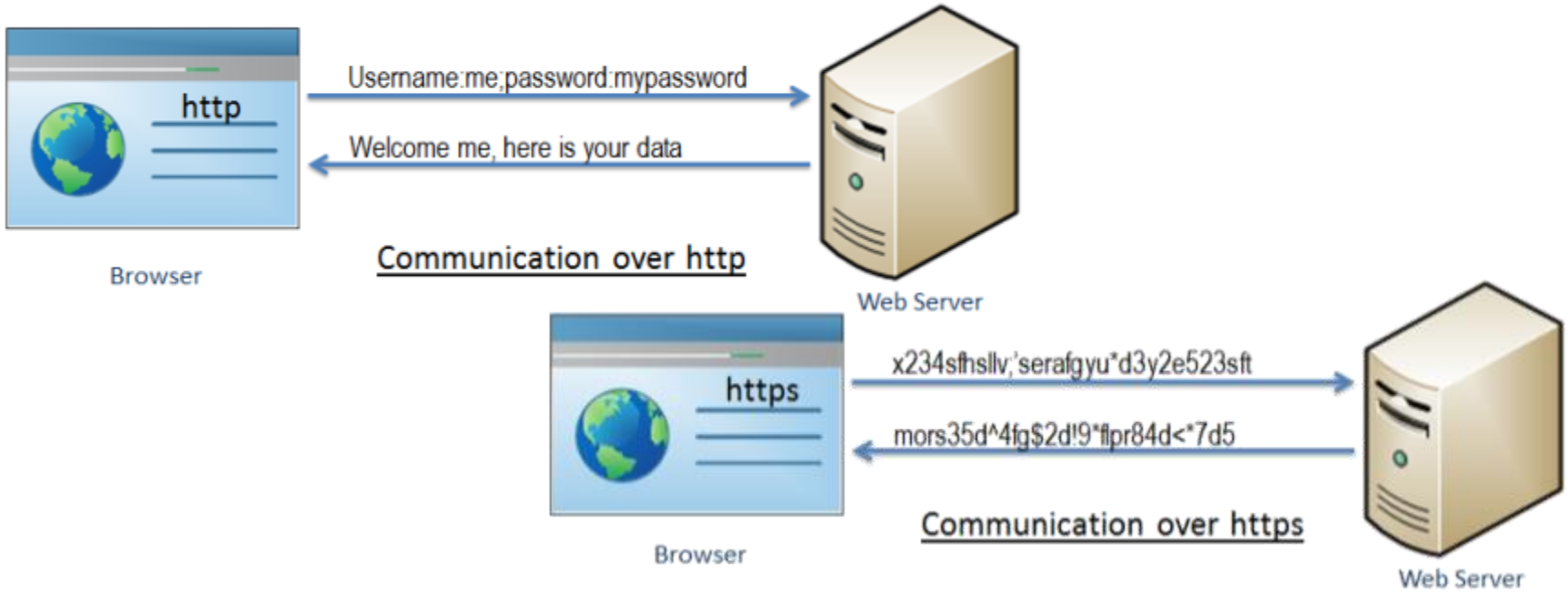
Protocolos: Caminho dos Dados



Comunicação SSL/TLS



- Comunicação por meio do HTTPS
- HTTP + TLS (*Transport Layer Security*)
  - Criptografa as informações ponto-a-ponto
  - HTTPS, por si só, não significa segurança total



ATIVIDADE

Atividade

- Discussão – Grupos – 15 minutos
- 1) Escolha uma empresa que atua online. Discuta com seu grupo quais são os principais tipos de dados que ela deve proteger e qual o impacto de perdê-los.
  - Elabore uma lista com 3 principais
- 2) Do conhecimento (trabalho ou pessoal), quais são os serviços de rede mais usados?
  - Elabore uma lista com 3 itens

ENCERRAMENTO

Resumo e Próximos Passos

- Noções básicas de plano de segurança
- Noções de redundância e backup
- Noções do funcionamento da rede

- **Pós Aula**: Aprenda Mais, Pós Aula e Desafio!
  - No padlet: https://padlet.com/djcaetano/segciber

- Equipamentos básicos da rede
- Vulnerabilidades comuns

PERGUNTAS?