

# FORUM IX.br - Salvador

28 e 29 de setembro 2017

REALIZAÇÃO:

**nic.br**

Núcleo de Informação  
e Coordenação do  
Posto BR

**cgi.br**

Comitê Gestor da  
Internet no Brasil



PATROCÍNIO PRATA:

**BRDigital**  
Telecomunicações

PATROCÍNIO BRONZE:



**BRDEFENDER**  
Tecnologia e Segurança

**LinkaBR**

**PROBAHIA**  
ASSOCIAÇÃO DE PROVEDORES DE INTERNET



UPBA

APOIO:

**STI**

Sistema Estadual de  
Tecnologia da Informação | UPEA



RNP

# Troubleshoot em Redes e Sistemas

## Minicurso WTR 2017

Jundaí Abdon, Bruno Ramos e Ibirisol Fontes  
PoP-BA/RNP

- **Tecnologia no dia-a-dia**
- **Tecnologias costumam falhar**
- **Constante troubleshooting em TI**
  - Fundamentos gerais de troubleshooting
  - Foco em redes
  - Ferramentas para tratamento
  - Muitas dicas e boas práticas

**Troubleshooting** é a 'arte' de resolver problemas. É uma busca sistemática e lógica pela raiz de um problema, de modo a que possa ser resolvido e o produto ou serviço retorne a execução de sua função original.

O termo Troubleshoot é composto pela junção de duas palavras do inglês, 'trouble' que significa 'problema' e 'shoot' que significa 'atirar'.



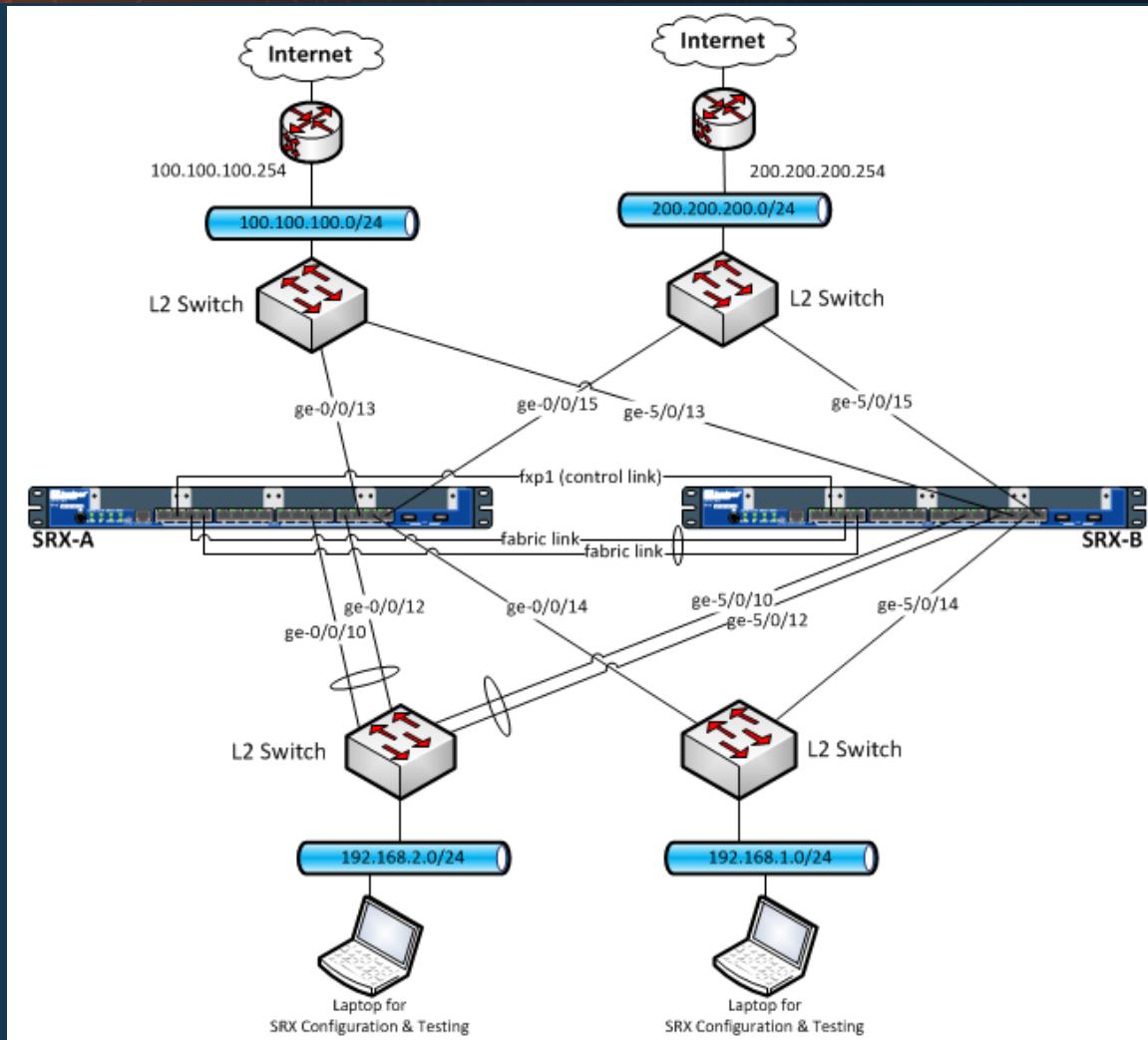
- **Passos globais para resolução de problema:**
  - 1. Analisar
  - 2. Encontrar
  - 3. Resolver
- **O que varia:**
  - 1. O problema
  - 2. O ambiente
  - 3. A solução

O **problema** é o que parou de funcionar

O **ambiente** é o conjunto de dispositivos, processos e fatos coletados após análise

A **solução** é a abordagem para se resolver o problema

# Uma pequena topologia

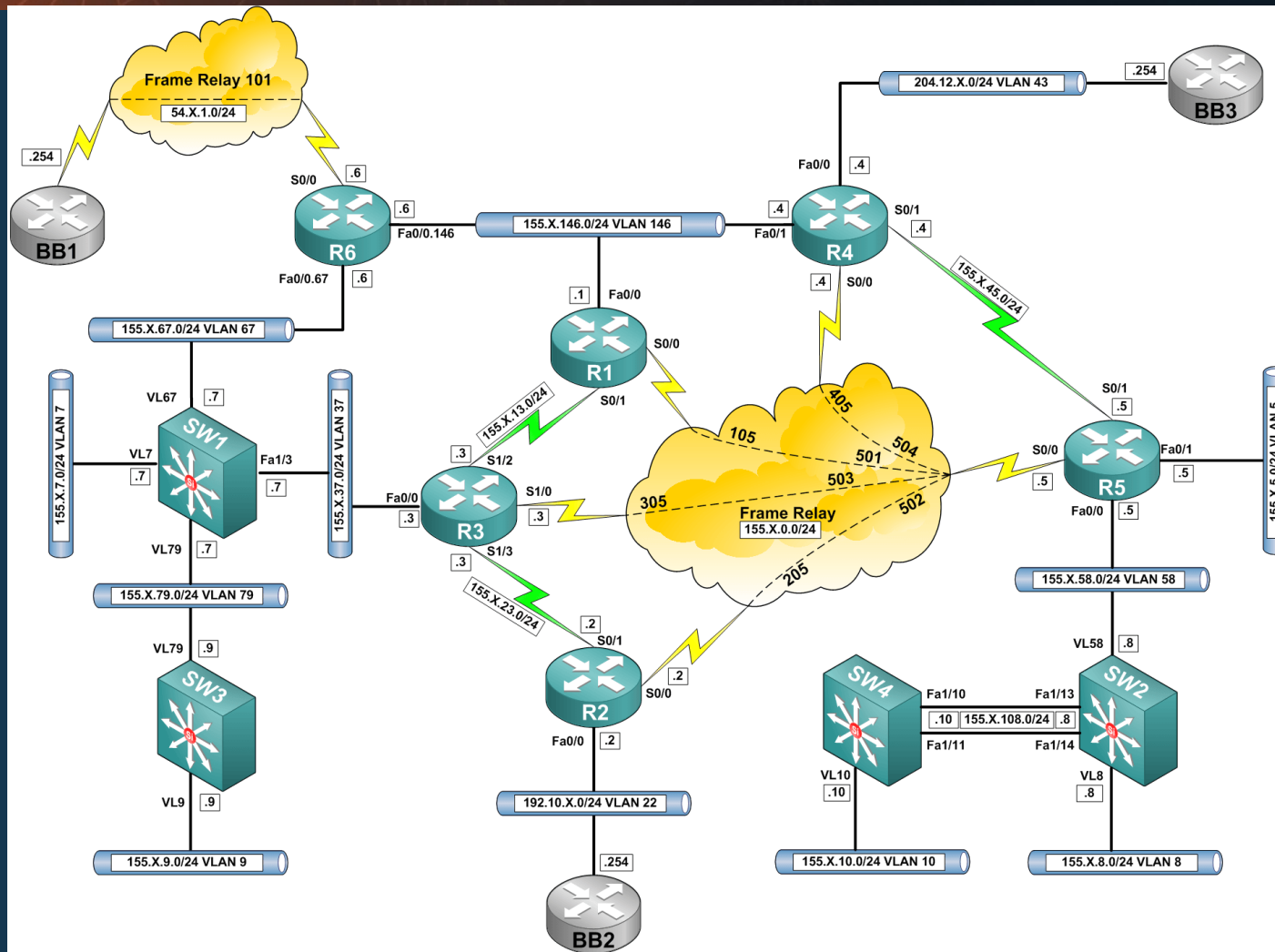


High Availability - SRX LAG & Dual Fabric Configuration

Fonte: <http://jncie-sec.exactnetworks.net/2012/11/high-availability-srx-lag-dual-fabric.html>



# Uma outra topologia



BGP troubleshooting – route not installed

Fonte: <http://lostintransit.se/2011/02/12/bgp-troubleshooting-route-not-installed/>

# Fluxo Estruturado de Troubleshooting

## **Passo 1:** Definir Problema

Documentar os Sintomas

## **Passo 2:** Coletar Informações

Reunir Fatos

## **Passo 3:** Considerar Possibilidades

Criar Hipótese

## **Passo 4:** Criar Plano de Ação

Criar Plano de Retorno

## **Passo 5:** Realizar Plano de Ação

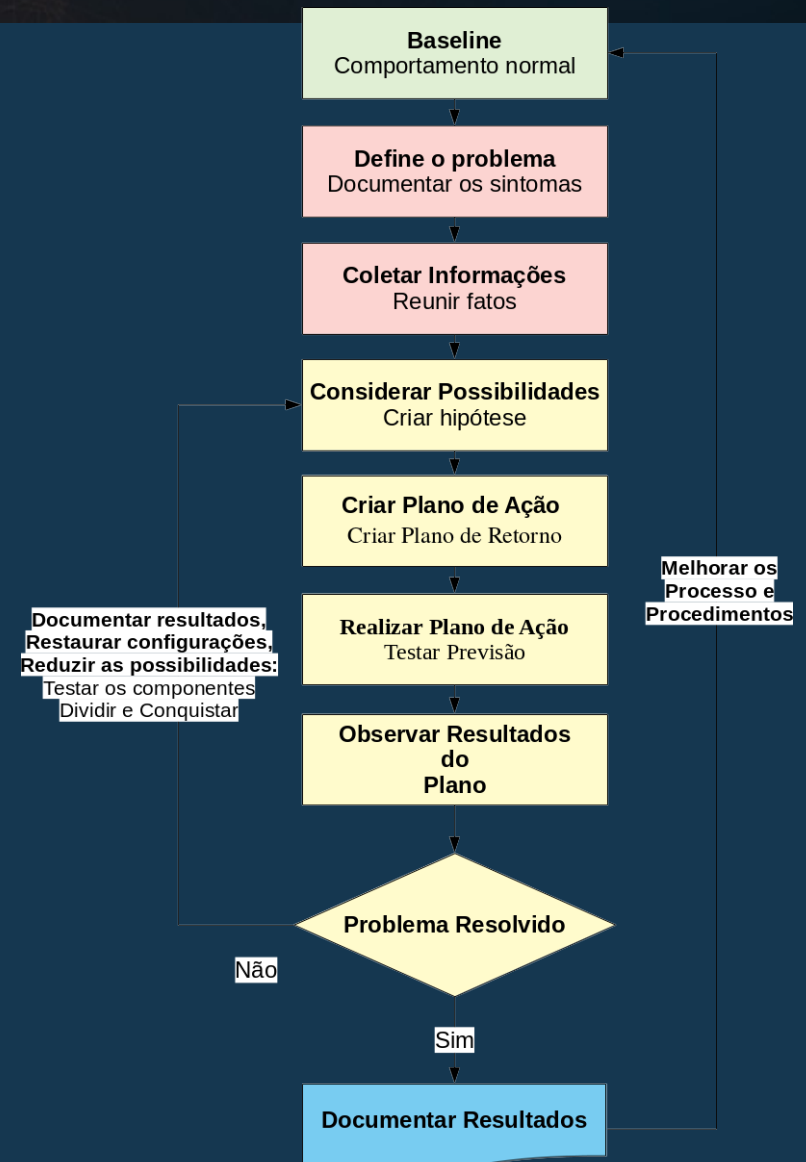
Testar Previsão

## **Passo 6:** Observar Resultados do Plano

Resolvido

Mantido, reverter o cenário

## **Passo 7:** Documentar Resultados





# Exemplo simples Troubleshoot

- **Problema reportado ou notado:**
  - Clientes sem acesso à um serviço na Internet
- **Qual a criticidade do problema?**
- **Definindo as variáveis envolvidas:**
  - Quem e quantos reclamaram?
    - O acesso já foi feito antes?
    - Quão recorrente é o problema?
  - Quais dispositivos estão envolvidos?
    - Switches, access points  
notebooks, celulares e computadores
  - Problema isolado ou geral?
    - Outras redes ou locais enfrentam o mesmo problema?

- **Definidas as variáveis, é preciso confirmar se o problema existe**
  - Checar ferramentas de monitoramento (se estiver monitorado)
  - Acesso remoto ou sensor de monitoramento (visão do cliente)
  - Teste do técnico no local (imediato para problemas sem acesso)
- **Identificar causa(s) do problema**
  - É possível alcançar destinos na internet através de outras redes?
  - Equipamentos ligados?
  - Cabos devidamente conectados?
  - Houveram modificação recente na rede?
  - Algum serviço da cadeia não esta funcionando corretamente
    - DNS, Firewall, proxy/cache, etc...
  - Queda elétrica recente?
  - Acesso remoto impossibilitado?
  - Logs apresentam mensagens de erros/alarmes?

- **Dada a causa do problema, possíveis abordagens de solução**
  - Troca/reparo de ativos envolvidos
  - Auxiliar o usuário
  - Não substituir ativo, reposicionar/remanejar os atuais
  - Ativar contingencia
  - Reconfigurar ativo
  - Reverter alterações não validades
- **Relatório completo sobre o problema e como foi / será resolvido**

- **Resultado final é falta de algo:**
  - Procedimento
  - Treinamento
  - Recursos
  - Conjunto de expectativas
  - Manutenção
  - Conhecimento
  - Planejamento
  - Etc
- **Reconhecer o papel humano em falhas de sistema**
  - Não quer dizer que a intenção é achar 'o' culpado
  - Muito menos punir...

## Não existe receita de bolo!

### Bolo de Aipim (macaxeira, mandioca)

#### Ingredientes:

750 ml. de leite ■ 1/2 kg de aipim ralado ■ 1 pacote de coco (opcional)  
2 colheres (sopa) de margarina ■ 4 ovos ■ 1 pitada de sal ■ 300 gr. de açúcar

#### Como fazer:

Retire os fios do aipim, e esprema o aipim depois de ralado para retirar o excesso de líquido. Coloque todos os ingredientes no liquidificador e deixe misturar bem. Pré-aqueça o forno. Unte a forma com margarina. Coloque para assar em forno médio por cerca de uma hora, até ficar dourado encima.

Para conservar melhor em dias quentes, guarde o bolo na geladeira.

kandisdesign.blogspot.com



Fonte: Mario Rodrigues  
(<https://mdemulher.abril.com.br/receitas/bolo-de-aipim/>)

- Saber os caminhos a se tomar é a 'arte'
- Existem vários problemas e vários caminhos para resolvê-los
- Com base no resultado das análises, pular para abordagem de melhor retorno
- Ser adaptável
  - Excluir possibilidades ao longo do caminho



# Estabelecendo os caminhos: Economia envolvida

- **Limitações em achar e resolver o problema:**
  - Tempo, conhecimento, custos
- **Custo:**
  - Tempo de conserto (homem/hora)
  - Custo monetário (substituição, aquisição)
- **Custo x Benefício entre compra e conserto**
- **Troubleshooter:** Descubra o que está errado e quanto custa para consertar
- **Economia:** Dita os recursos ao alcance e influencia na viabilidade das soluções



Fonte: Andrew Magill (<http://flic.kr/p/68vjKV>),  
license: Creative Commons (CC BY 2.0)

- **Administradores de rede gerenciam redes para outros agentes**
  - Instituição
  - Gestores
  - Companheiros de trabalho
  - Clientes
  - Terceiros



- **Isso exige boa gestão de comunicação**
  - Se comunicar corretamente com os pares e agentes
  - Sistemas para registros de eventos, comunicados, manutenções, chamados
  - Informações sobre ações que impactem na rede ou serviços devem ser propagadas com antecedências
  - Transparência e clareza



- **Substantivos inespecíficos**
  - “Não quer ligar” – O que? Quando?
- **Verbos inespecíficos**
  - “Ela desligou o computador” – Como especificamente?
- **Comparações**
  - “O site está lento” – Comparado com o que?
- **Julgamentos**
  - “Óbvio que a baixa voltagem – Quem fez o julgamento causou a falha” e com que presunções?

- **Nominalização - verbos em substantivos**
  - “A investigação da falha de rede não deu resultado”
  - Quem investigou o quê? – Como conduziram a investigação?
  - Quais as conclusões?
- **Modal de possibilidade ou necessidade**
  - “Eu não posso fazer o servidor ligar”
  - “Você deve ligar a bateria de backup antes de iniciar”
  - O que aconteceria se ...? O que te inibe de...?
- **Quantificadores universais**
  - “Isso nunca funciona!” – Alguma vez já funcionou?

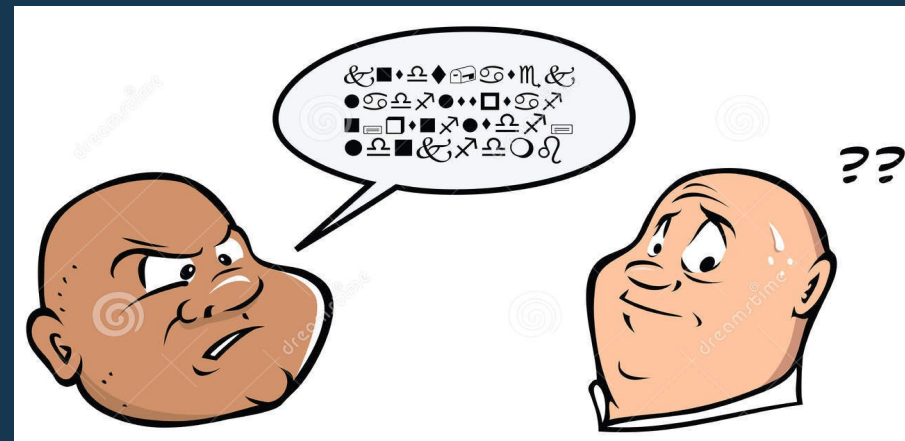
- **Equivalência complexa**
  - “Pessoal está em intervalo. A produção está parada”
  - Como os trabalhadores pararem significa a produção parar?
- **Pressuposições**
  - “Fique atento ao nível de tráfego da rede”
  - O que te leva a pensar que ...?
- **Leitura da mente**
  - “Bruno não liga e não vai nos ajudar com o debug da rede”
  - Como exatamente você sabe disso?



- **Causa e efeito**

- “Ficaria ligado, mas bateria do nobreak estava baixa”
- “Apesar de passar nos testes TCP, o circuito está ruim, pois não consigo acessar quase nenhum site.”
- Como isso causa aquilo? O que não causaria aquilo?
- Já existiu situação em que A não implicou em B?

- Um bom troubleshooter tem uma dose de ceticismo!
  - Sabe filtrar as informações ocultas nas mensagens
  - Capacidade de extrair informações necessárias para debugging do problema



# Pontos de partida para identificação de problemas



- Checagens de sanidade de configurações
- Auditorias e manutenções de rotina
- Monitoramento
  - Logs
  - Alarmes
  - Gráficos

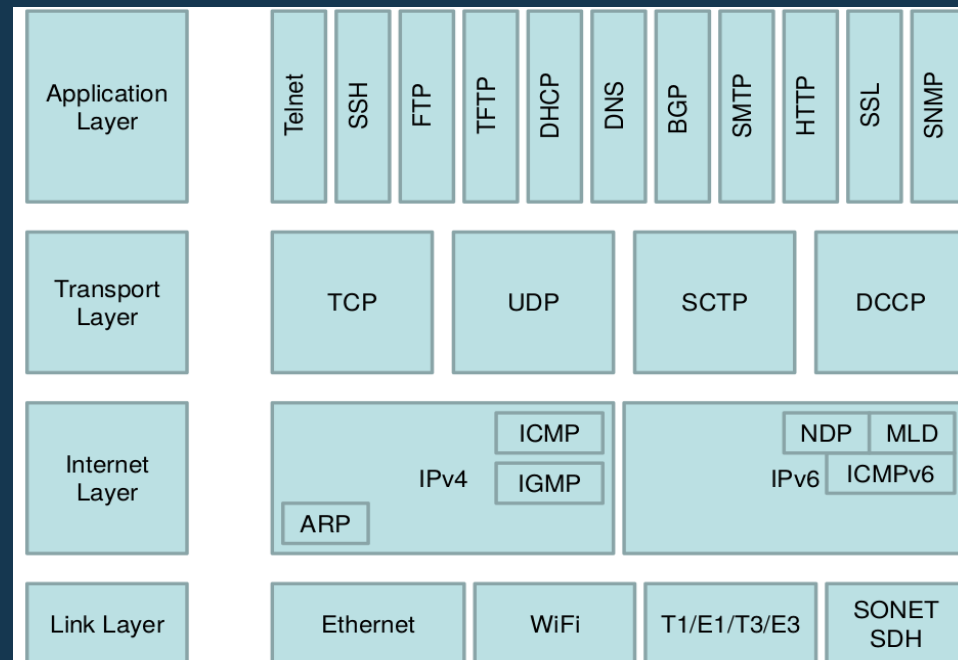
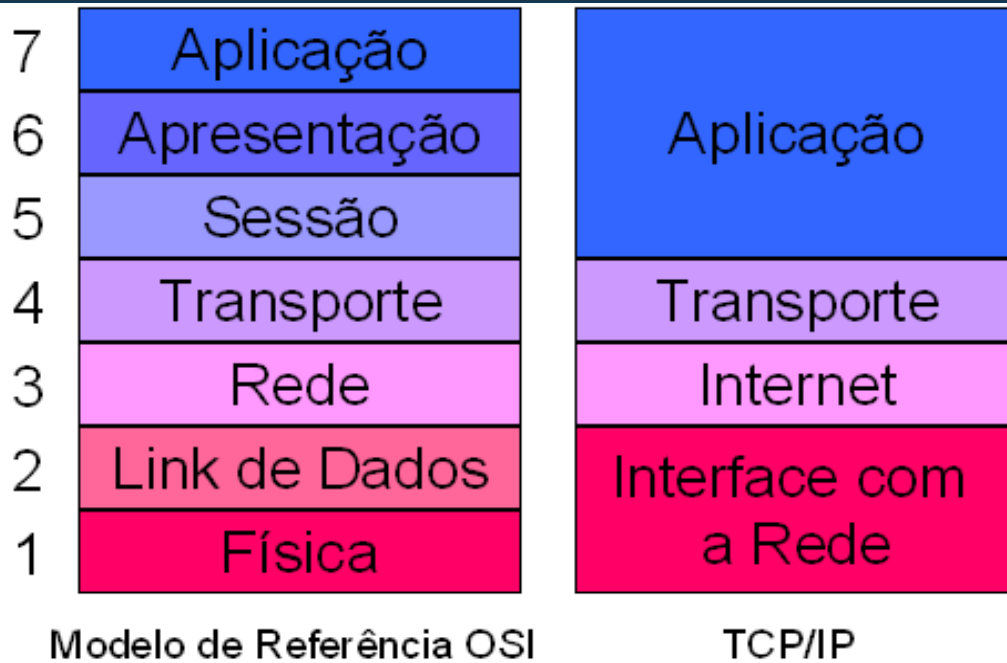
- Informações do report do problema
- Duplicação do problema
- Por onde os gráficos ficam anormais
- Começar investigação pelas mudanças recentes do ambiente
- Logs e mensagens de erro
- Documentos de manual ou suporte técnico
- Ordem das coisas

- **Saber que 'A' vem antes de 'B' pode te poupar tempo no troubleshooting**
  - 'A' estar ou não funcionando influencia no resultado do teste em 'B'
  - Conhecer fluxo das camadas de rede
  - Conhecer fluxo de regras de firewall
  - Ordem de inicialização de equipamentos, máquinas virtuais, módulos, linhas de comando, softwares, scripts, etc
  - Ordem das configurações e seus parametros



- **Estratégias comuns em camadas:**
  - Isolar camadas durante troubleshooting
    - Debug completo de link
      - Começar pela camada 1
    - Debug específico de aplicação
      - Começar pela camada 7
    - Dividir para conquistar
      - Começar pela camada 3

# Especificamente sobre camadas de rede



# Temos uma ideia dos passos iniciais...

FORUM  
**IX.br - Salvador**

28 e 29 de setembro 2017

## E como resolver?

- **Hardware**
  - Temperatura
    - Fans
    - Temp do ambiente e do CPU
  - Processamento
    - Porcentagem de uso
    - Não agregar todos os serviços em um ativo
    - Replanejar e distribuir carga / serviços
- **Dica: monitore todos!**
- **Memória**
  - Não deixar cair na swap
- **Armazenamento**
  - Não usar apenas uma partição em sistema crítico

- **Software**
  - Instalações e configurações padrão
    - Usuários e senhas
    - Serviços, módulos e plugins não utilizados consumindo recursos
  - Vulnerabilidades
  - Problemas de escalabilidade
  - Não observar recomendações do fabricante
  - Upgrades “a quente”

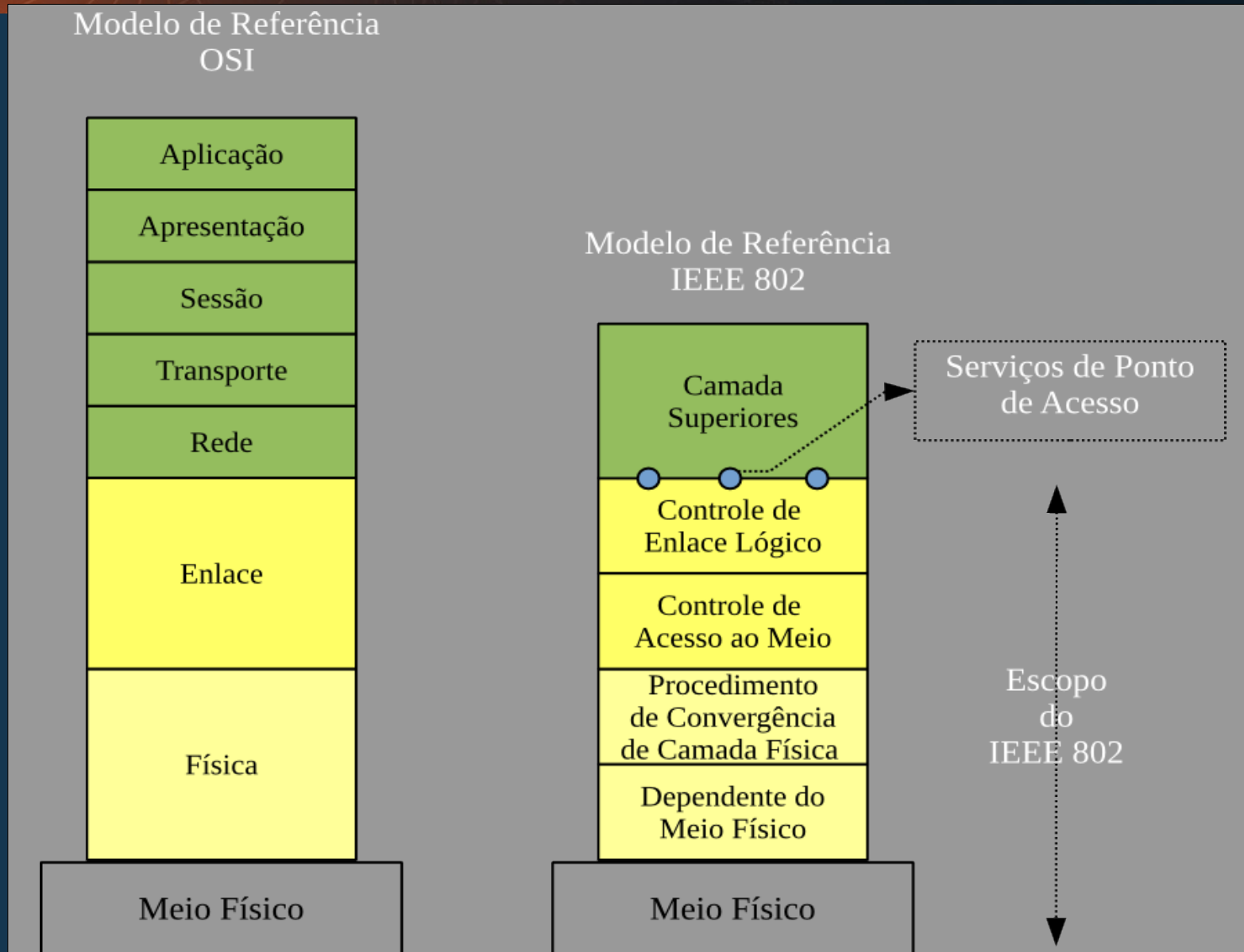
- **Hardware:**
  - Taxa de I/O e saúde do HD:
    - iotop
    - smartctl
  - Processamento e memória
    - htop
    - vmstat
    - smem
  - Temperatura
    - sensors



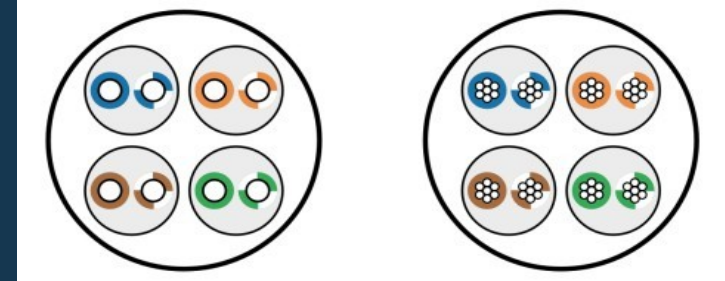
- **Software**
  - Detalhe execução
    - strace
  - Logging
    - syslog-ng
    - Rsyslog
- **Ferramentas de monitoramento e alarmes:**
  - Cacti    – Zabbix    – Icinga    – Nagios    – Gnokii

- **Versão de softwares e firmwares**
  - Verificar recomendação do fabricante e ler changelogs
  - Se possível testar atualizações em memória secundária ou ambiente controlado
  - Upgrade imediato para novas versões apenas se:
    - Corrigir bugs críticos e falhas de segurança ou;
    - Implementar funcionalidade essencial pra a rede
- **Configurações default**
  - Sempre modificar / customizar configurações e parâmetros
  - Observar funcionalidades precisam ser desabilitadas
  - Ler documentações de hardening
- **Garantir processo de rollback em configurações e equipamentos**
- **Não confiar apenas em terceiros (fornecedores)**
- **Atenção para versões estáveis de software!**

# Problemas Comuns - Camada Física



- Cabeamento
  - Blindagem
    - Magnética e roedores
  - Distância e atenuação
    - Adaptadores e emendas
    - Tipo GBIC
    - Sujeira na fibra
    - Clivagem
- Interface ou módulo com defeito
- Interface com muito tráfego



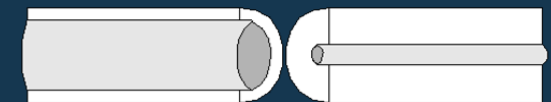
Visão interna de um cabo sólido e de um cabo stranded



**Angular Misalignment**



**Core Diameter Mismatch**

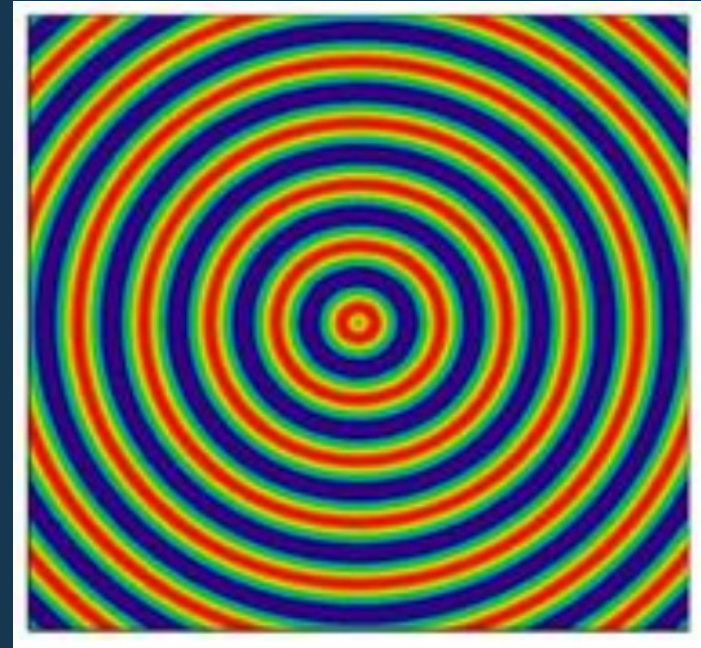
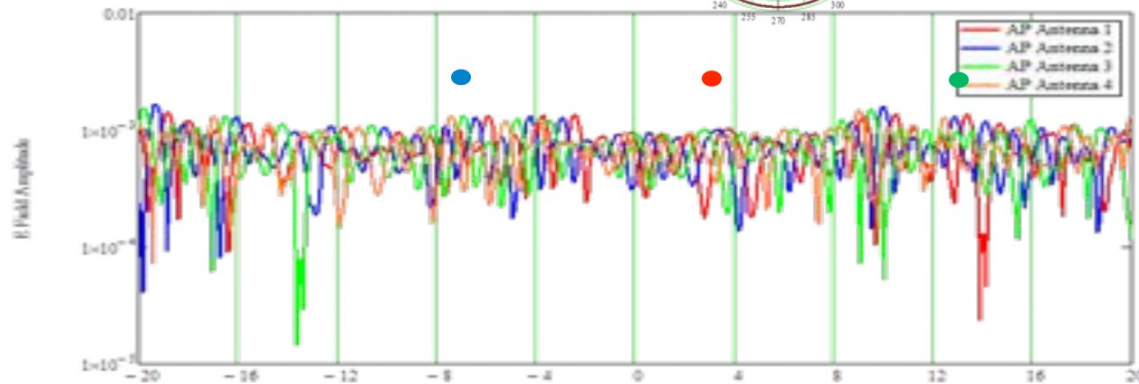
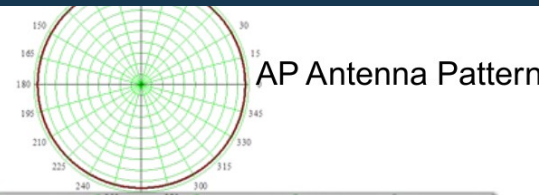


Visão interna da clivagem e tamanho de núcleo de fibra

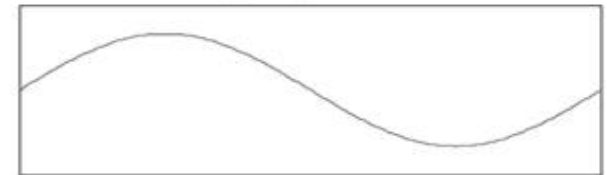


- Rede Wireless
  - Distância e atenuação
  - Free space loss
  - Ruído

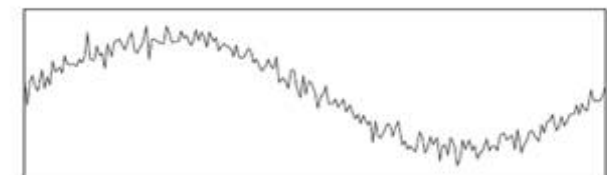
Room Width: 10m  
Room Length: 10m  
Room Height: 7m



Sinal Analógico Original

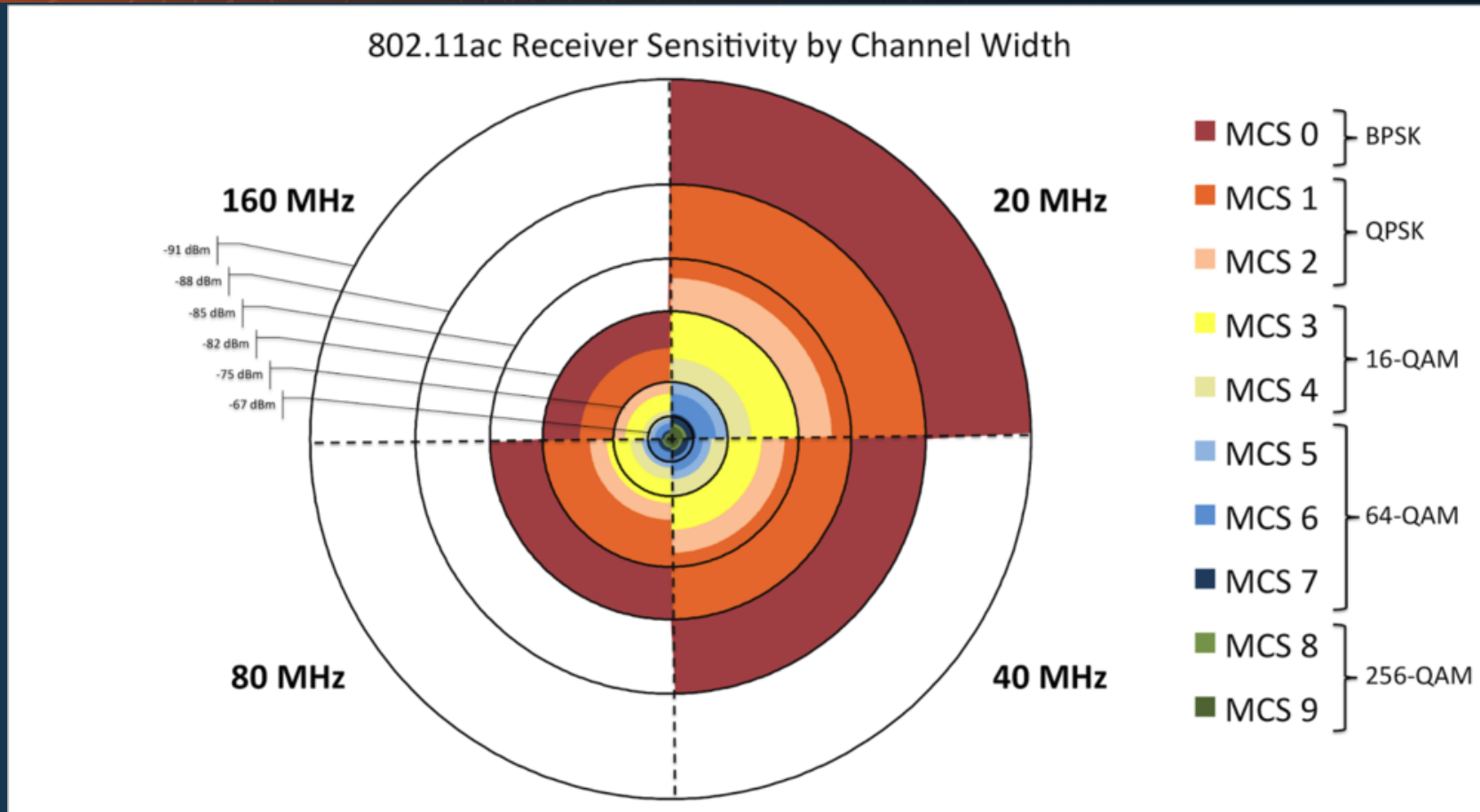


Sinal após adição de ruído





# Problemas Comuns - Camada Física



802.11ac Receiver Sensitivity (Down to -91 dBm)

Fonte: <http://www.revolutionwifi.net/revolutionwifi/2014/08/80211ac-receiver-sensitivity.html>

- Rede Wireless

- Interferência Multicaminho

- Difração
    - Refração
    - Ocultamento
    - Perda propagação

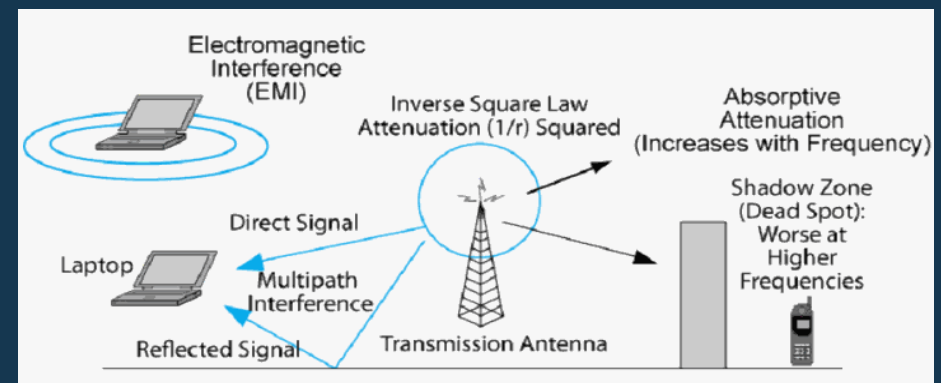
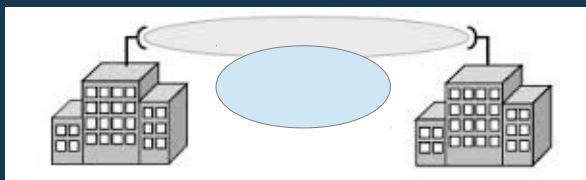
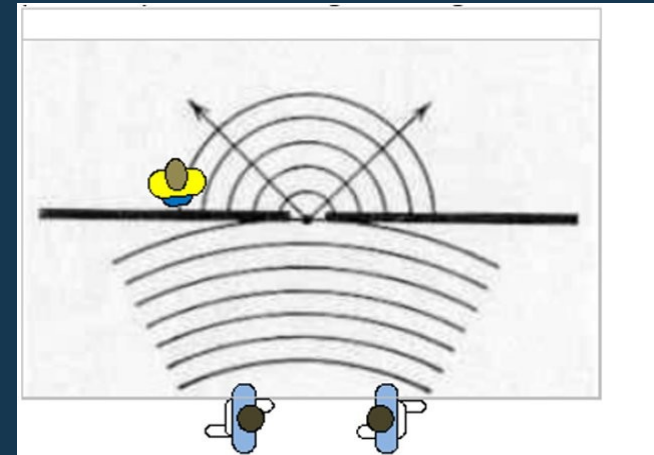
- LOS

- Zona Fresnel

- SINR (Interferência)

- Modulação sinal

- Banda da rede wireless





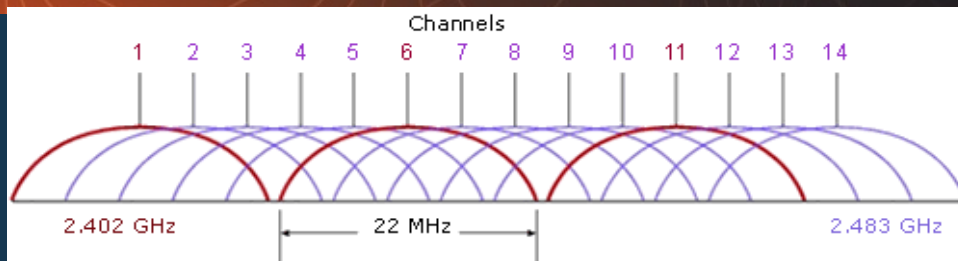
- **Rede Wireless**

- Ganho e intensidade do sinal da antena
  - Direcional    • Omnidirecional
- Sensibilidade mínima de antena
  - Placa de rede típica: -95db
- Intensidade de sinal do cliente ao AP
- Planejamento do posicionamento dos APs
- Espectro sobrecarregado
  - Sobreposição de canais
- Rogue AP

# Problemas Comuns - Camada Física

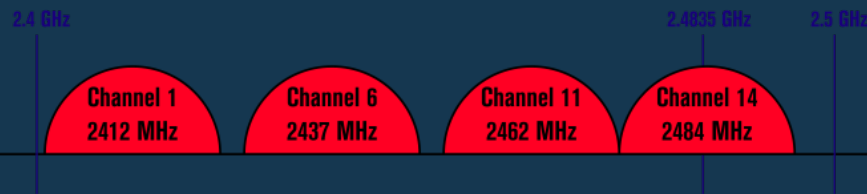
FORUM  
IX.br - Salvador

28 e 29 de setembro 2017

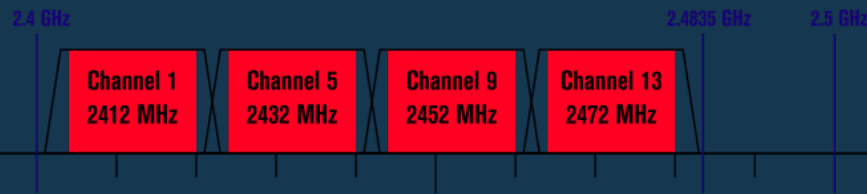


## Non-Overlapping Channels for 2.4 GHz WLAN

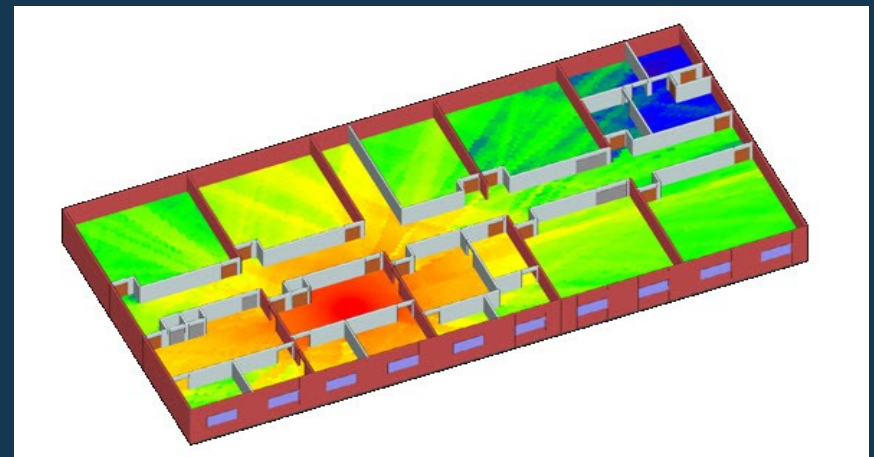
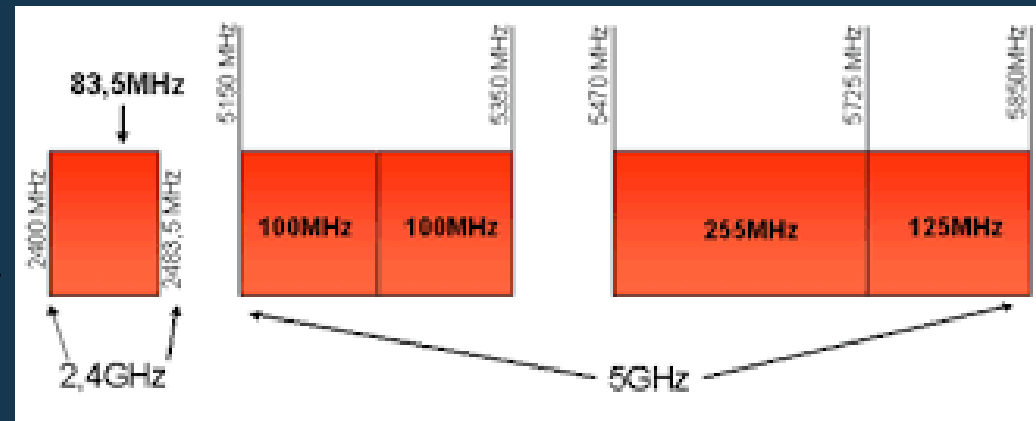
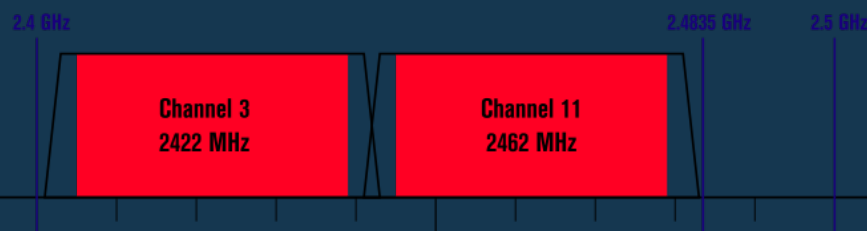
802.11b (DSSS) channel width 22 MHz



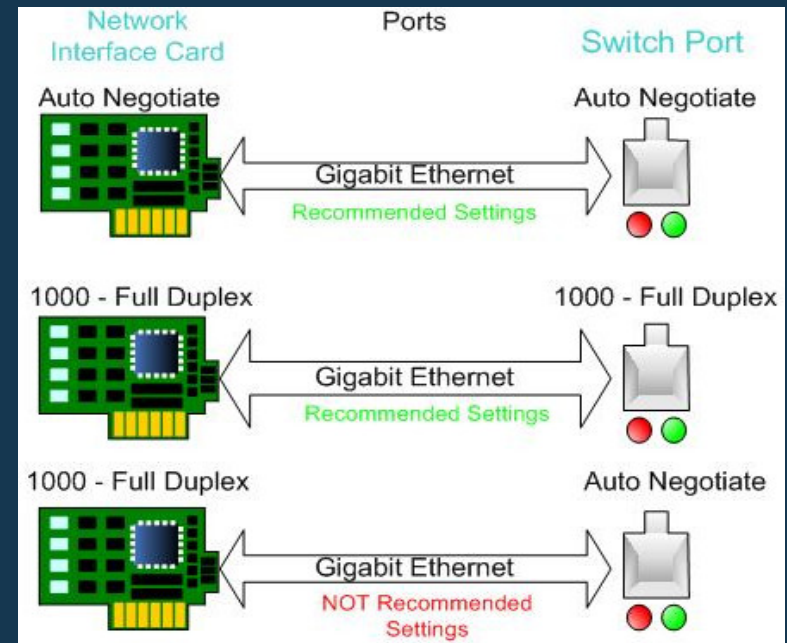
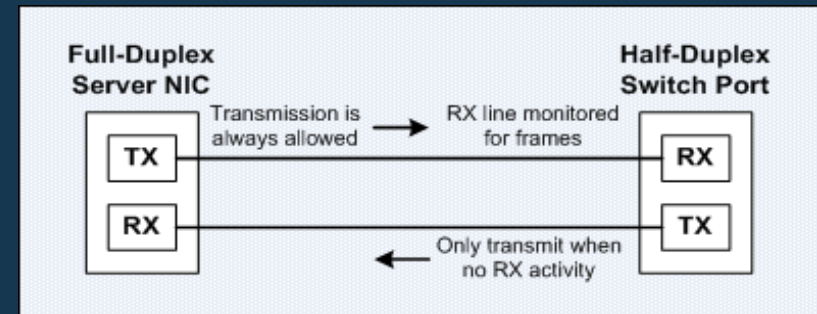
802.11g/n (OFDM) 20 MHz ch. width - 16.25 MHz used by sub-carriers



802.11n (OFDM) 40 MHz ch. width - 33.75 MHz used by sub-carriers



- Auto negociação
  - Duplex mismatch
  - Auto e Full-Duplex manual
  - Problemas em tráfego TCP
- Dica: auto negociação habilitada!
  - Principalmente Gigabit



- Comportamento esperado de interfaces conforme padrões:

Padrão	Ano	Velocidade	Cabo	Auto negociação
802.3i	1990	10M	Par trançado	Sem auto-negociação
802.3u	1995	10/100M	Par trançado	Opcional, não confiável
802.3-1998	1998	100/100M	Par trançado	Opcional
802.3ab	1999	10/100/1000M	Par trançado	Opcional @ 10/100M Requerido @ 1Gbps

- **Interface Gigabit**
  - Comportamentos de interfaces Giga em auto negociação:

Auto-negociação habilitada	Status Link A   Link B
Ambas	UP   UP
A	DOWN   UP
B	UP   DOWN

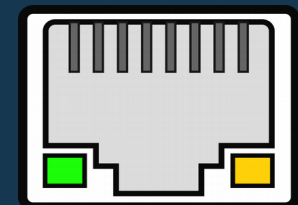
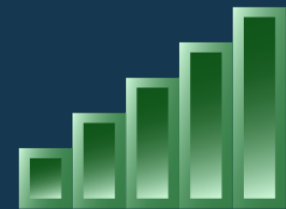
- **Link status (GNU/Linux)**

- Verificar:

- mii-tool
    - ip link show <iface>
    - iw dev <w\_iface> link
    - iwconfig

- Modificar:

- ip link dev <iface> set up ou down
    - ifconfig <iface> up ou down





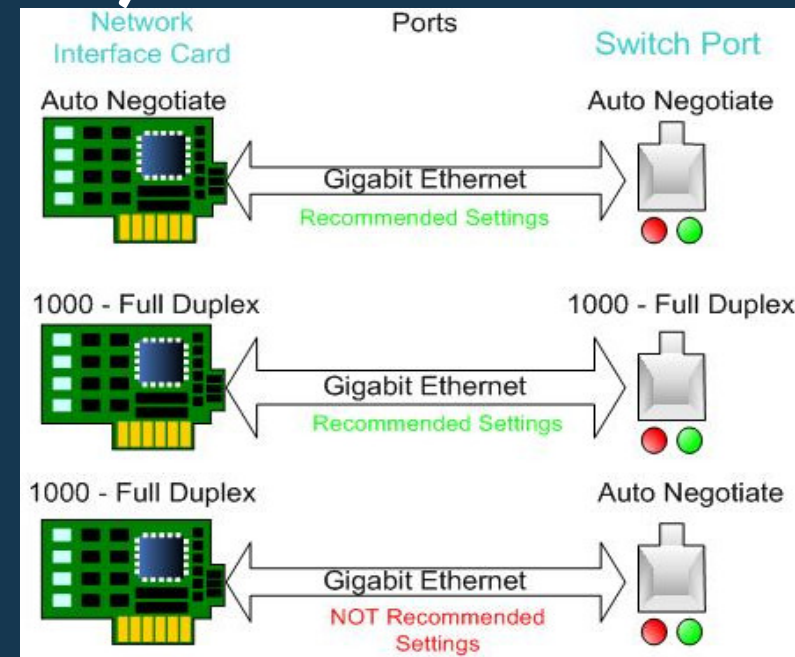
- Autonegociação (GNU/Linux)

- Verificar:

- mii-tool
    - ethtool <iface>

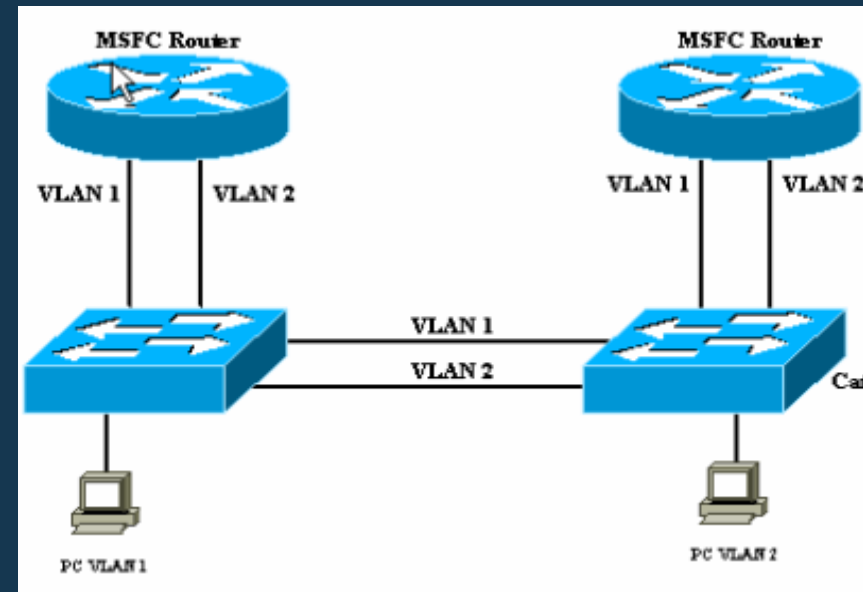
- Modificar:

- ethtool -s <iface> autoneg on
    - ethtool -s <iface> speed 100 duplex full autoneg off
    - mii-tool -F 100baseTx-FD <iface>





- **VLAN**
  - Não enxergar MAC de vizinhos
  - tag vs untagged
- **MAC**
  - Estouro de tabelas
    - CAM e TCAM
    - FDB
  - Duplicação de MAC
- **Flags de erro (CRC, etc)**
  - Podem sugerir duplex mismatch
- **Broadcast Storm (topologias multicaminho)**



- MTU / Fragmentação
  - PMTUD
  - Jumbo Frame
    - $1501 < \text{MTU} < 9000$

Protocol	Undersized PMTU	Oversized TCP MSS	Undersized TCP MSS	PMTUD failure
IPv4	<b>PMTU &lt; 576 bytes</b> IP fragmentation for UDP packets; critical in DNS servers	<b>MSS &gt; PMTU – 40 bytes</b> Will trigger a Can't Fragment ICMP from the first TCP packet	<b>MSS &lt; 1380 bytes (except DNS)</b> Will generate extra packets increasing per packet processing.	Large packets that have DF bit set can potentially always be dropped (pmtu black holes)
IPv6	<b>PMTU &lt; 1280 bytes</b> Violation of IETF standards; packets will be dropped	<b>MSS &gt; PMTU – 60 bytes</b> Will trigger a Packet too Big ICMP from the first TCP packet	<b>MSS &lt; 1220 bytes (except DNS)</b> Will generate extra packets increasing per packet processing.	Large packets can potentially always be dropped (pmtu black holes)

- MTU (GNU/Linux)

- Verificar:

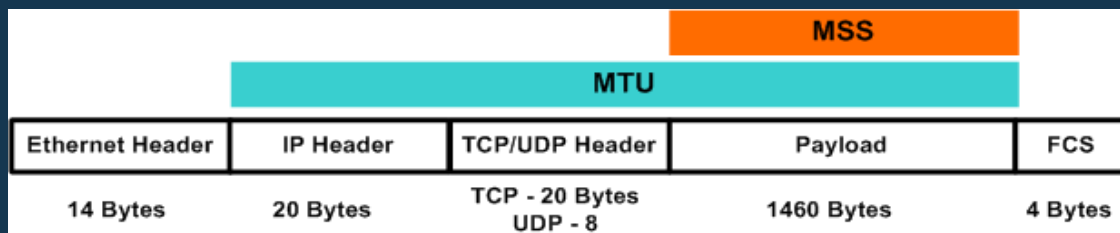
- ifconfig <iface>
    - ip link show dev <iface>
    - tracepath -n -m <hops> <destino>
    - Bônus

- Em sistemas Windows:

- netsh interface ipv4 show subinterfaces

- Modificar:

- ip link set dev <iface> mtu <MTU>
    - ifconfig <iface> mtu <MTU>



- **IP ou máscara incorretas**

- IP duplicado

- **ARP**

- Spoofing / Poisoning

- MAC Flooding

- **DHCP mal configurado**

- **Rotas**

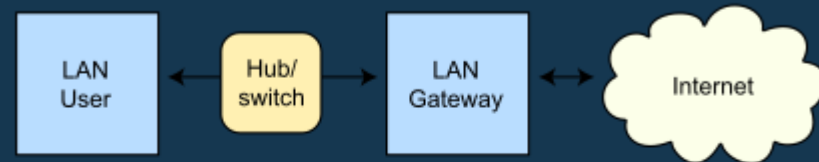
- Estáticas

- Dinâmicas / Importadas

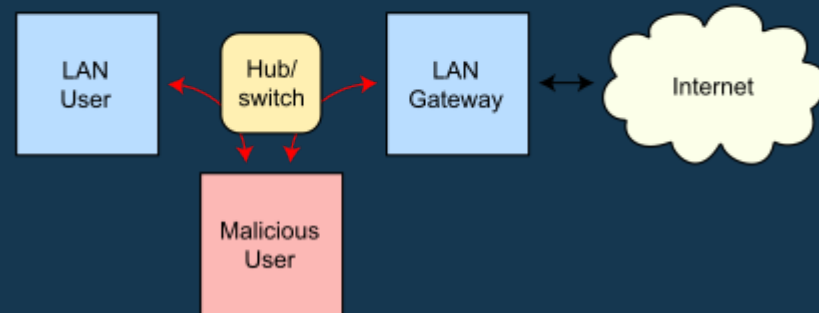
- BGP, OSPF

- **DNS mal configurado**

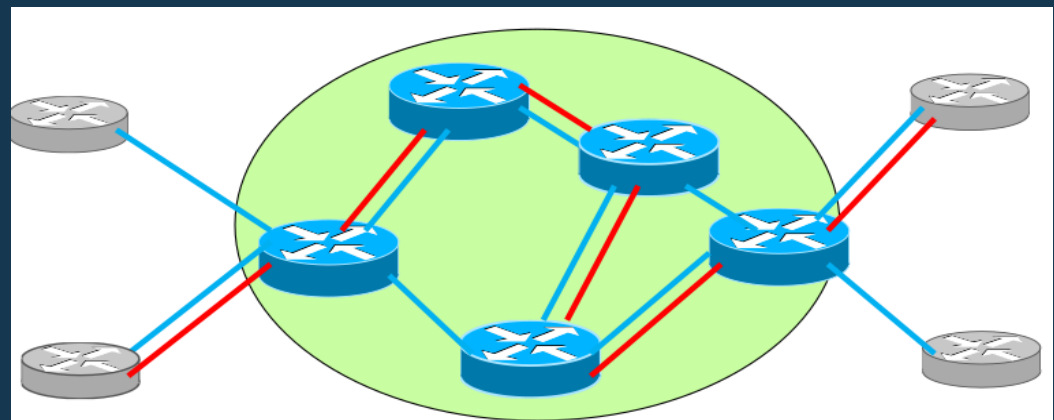
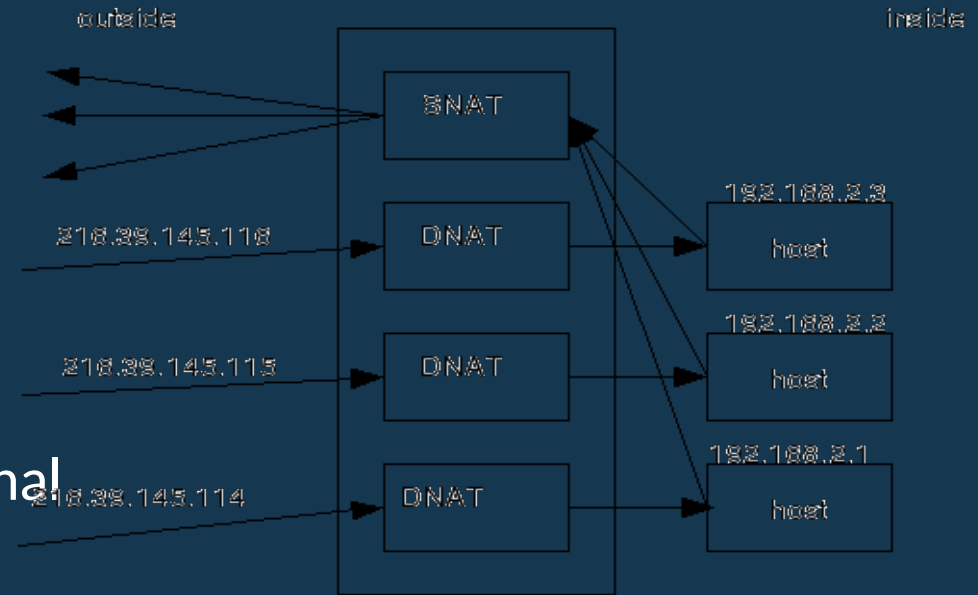
Routing under normal operation



Routing subject to ARP cache poisoning



- IPv4
  - SNAT e DNAT
    - Overhead recursos
- IPv6
  - Endereço hexadecimal
  - IPv6 habilitado, mas não funcional
    - Router Advertisement
    - Delay resolução DNS
  - IPv6 sem firewall
  - Bloqueio de ICMPv6
    - PMTUD, ARP, RA, etc



- **ARP (GNU/Linux)**

- Tabela:

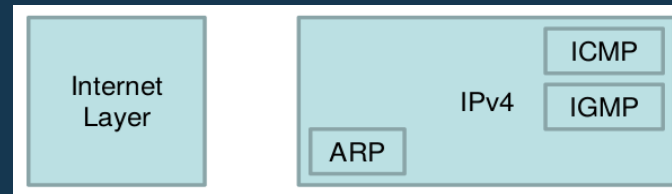
- `arp -n -i <iface>`
    - `arp -D <ip/hostname>`
    - `ip neigh show`

- Modificar:

- `arp -i <iface> -s <ip> <mac>`
    - `ip neigh add <ip> lladdr <mac> dev <iface>`
    - `arp -i <iface> -d <ip>`
    - `ip -s neigh flush all`

- IP Duplicado:

- `arping -D -I <iface> -c <probes> <seu-ip>`
      - Se houverem respostas, há IP duplicado na rede.





- Rotas (GNU/Linux)

- Tabela:

- ip route
- route -n

- Verificação estática:

- traceroute -n <destino>
- mtr -n -r -c <quantidade> <destino>
- mtr -w -c <quantidade> <destino>

- Verificação dinamica:

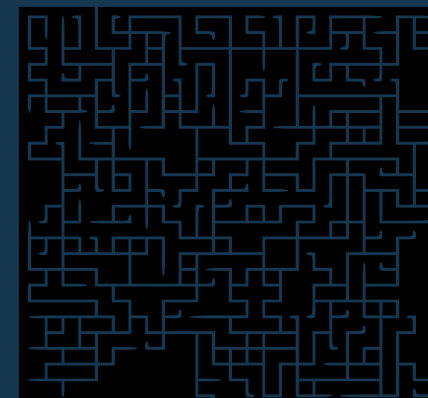
- mtr -n <destino>
- perdas no caminho, desvios e etc.

- Modificar:

- ip route add <subnet> dev <iface>
- ip route add default via <gw> dev <iface>
- ip route del <subnet> dev <iface>

Pingdom-ThinkPad (0.0.0.0) My traceroute [v0.82] Thu Jul 11 14:03:11 2013  
Keys: Help Display mode Restart statistics Order of fields quit

		Packets		Pings					
Host	Loss%	Snt	Last	Avg	Best	Wrst	StDev		
1. 172.20.10.1	0.0%	3	1.6	1.6	1.5	1.7	0.1		
2. 10.66.55.66	0.0%	3	60.7	58.6	57.2	60.7	1.9		
3. 10.66.55.65	0.0%	3	65.6	63.7	57.9	67.6	5.1		
4. 10.66.54.133	0.0%	3	67.7	63.3	58.4	67.7	4.7		
5. 10.66.56.6	0.0%	3	61.1	60.4	57.3	62.9	2.8		
6. 10.66.56.2	0.0%	3	66.6	62.6	59.3	66.6	3.7		
7. 80.251.201.34	0.0%	3	69.5	67.9	66.8	69.5	1.4		
8. te0-7-0-9.ccr22.sto03.atlas.cog	0.0%	3	64.0	62.4	57.4	65.8	4.4		
9. te0-0-1-3.ccr42.ham01.atlas.cog	0.0%	3	78.7	89.9	78.7	104.8	13.4		
te0-0-1-1.ccr42.ham01.atlas.cogentco.com									
te0-8-1-1.ccr42.ham01.atlas.cogentco.com									
10. te0-1-0-3.mpd22.ams03.atlas.cog	0.0%	3	83.3	79.7	75.9	83.3	3.7		
te0-6-0-3.ccr22.ams03.atlas.cogentco.com									
11. te0-4-0-0.ccr22.lon13.atlas.cog	0.0%	3	133.5	114.6	95.6	133.5	26.8		
te0-4-0-0.mpd22.lon13.atlas.cogentco.com									
12. te0-0-0-10.ccr22.jfk02.atlas.cog	0.0%	3	165.5	170.4	165.5	175.2	6.8		
13. te0-3-0-5.ccr21.jfk05.atlas.cog	0.0%	2	175.0	174.8	174.7	175.0	0.2		
te0-6-0-1.ccr21.jfk05.atlas.cogentco.com									
14. level3.jfk05.atlas.cogentco.com	0.0%	2	183.3	182.2	181.1	183.3	1.6		



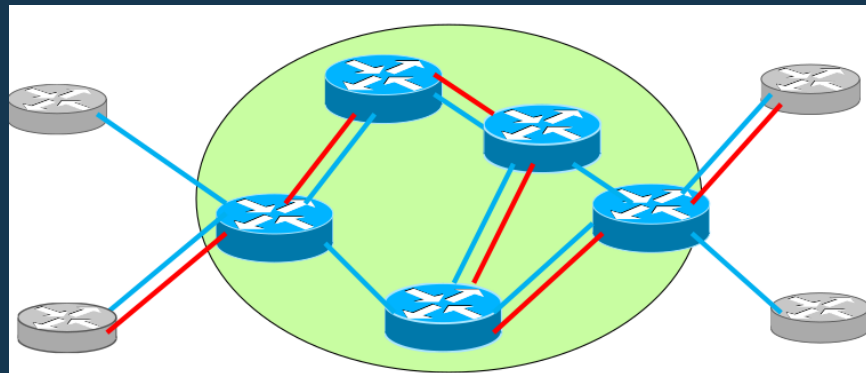


- **Mensagens Destination Unreachable**
  - Destination Host
    - Sistema local ou roteador remoto não tem rota para o host destino
    - Se mensagem for apenas “Destination Host Unreachable”, então não há rota no sistema local e os pacotes nem chegaram na rede
    - Resposta “Reply From <IP>: Destination Host Unreachable”, então um roteador de endereço <IP> informou que não tem rota

- **Mensagens Destination Unreachable (cont.)**
  - Fragmentation Needed and DF Set  
Indica que um pacote com o campo 'Não fragmente' habilitado no cabeçalho IP. Utilizado para descobrir o menor tamanho de MTU fim a fim via ping
- **Tempo Excedido**
  - Request Timed Out  
Indica que nenhum Echo Request foi recebido em 1 segundo.  
Talvez por congestionamento da rede, falha de ARP request, filtragem de pacote, erro de roteamento ou um descarte silencioso.

- **Quando não retorna nada?**
  - Drop no firewall
  - Host destino não tem rota correta para origem
    - Ou gateway default não configurado
- **Ferramenta de teste**
  - ping <IP ou nome>
  - traceroute, tracert, tracepath
  - PMTUD, scamper

- **Problema em link origem-destino**
  - Problema de camada 3 no primeiro hop
  - Problema camada 3 ao longo do caminho
  - Problema de resolução de nome
  - Problemas de camadas abaixo



# Problemas Comuns Camada de Transporte

- TCP

- MSS

- Ajuste necessário

- Túneis GRE, IP-IP, IPSEC

- TCP MSS clamping

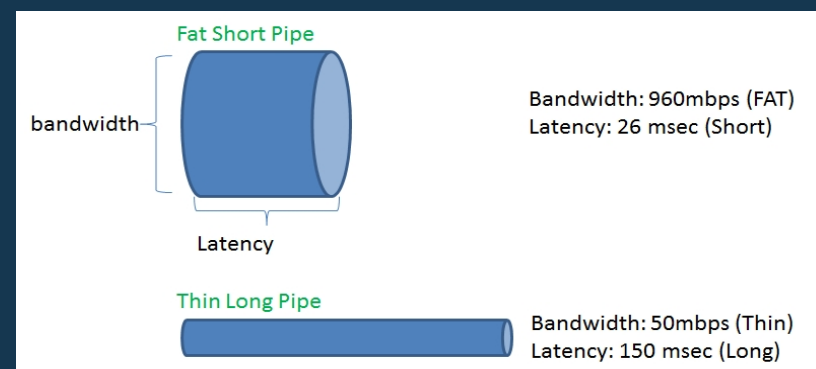
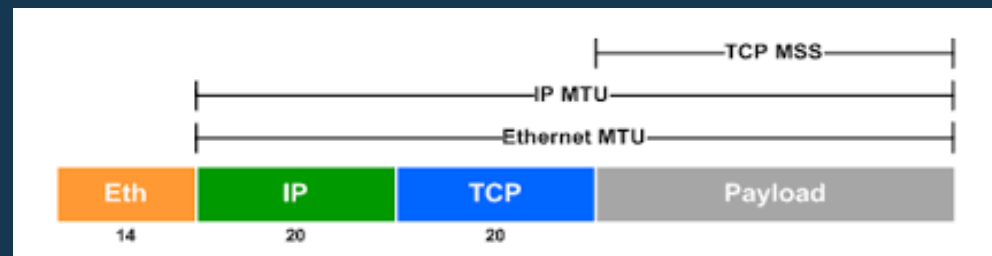
- TCP buffer

- Latência e largura de banda

- Alta reação à perda de dados

- UDP

- Rede congestionada



- Portas

- Porta fora do alcance

- Dispositivo não escutando

- **Scan de Portas**

- Verificar portas:
  - `hping3 -c 3 -S <IP ou nome> -p 80`
  - `telnet <IP ou nome> 80`
  - `nc -zv <IP ou nome> smtp`
- Verificar conexões UDP e TCP locais:
  - `netstat -atu`
- Informações de tráfego:
  - `iptraf`
  - `iftop -i <iface>`
- Escutar porta:
  - `netcat -l 4444`



- **Scan até host remoto**

- `nmap -A exemplo.com.br`

# Problemas Comuns - Lentidão no acesso

- À internet via IPv6
  - Habilitado na máquina origem e nos registros de DNS
  - Mas acesso à internet via IPv6 não funcional
- Alta latência
  - Distância
  - Congestionamento
    - Rede
    - Sobrecarga recursos
  - Perda de pacotes
    - Retransmissões TCP
  - Tempo resposta nas consultas DNS



Ping para o Google (8.8.8.8) tem dropado o pacotes

Latência (RTT) não está diretamente ligada à banda de link



- **Link saturado**
  - Tráfego válido, loop ou broadcast storm?
    - Identificação ainda é um desafio em alguns cenários
- **Alto consumo de recursos dos ativos de rede**
  - Processamento
  - Memória
  - Buffers e filas de interfaces

# Problemas Comuns – Roteamento

- Métricas mal definidas no roteamento dinâmico
- Rotas Default / Parcial / Full
- Rotas estáticas não observadas
- Loops no roteamento
  - A para B, C, D, C, D, C...
  - Estática / Dinâmico
  - TTL e seu amigo...
- Filtros de rotas/prefixos
- Assimetria no roteamento
- Configuração errônea com os vizinhos
  - Autenticação, mascara, tempo

# Problemas Comuns - Firewall, ACLs e QOS

- **Bloqueios ou prioridades para:**
  - MAC    – VLAN        – Filtro IP / Rede    – Portas
- **Firewall**
  - Regras muito específicas
  - Regra de drop antes regras de accept (virse-versa)
- **ACLs**
  - Ordem das ACLs
  - Duplicidade
  - Concorrência
- **Não tem como prever comportamento para redes fora do seu controle**
  - ICMP, drop, latência e rotas

- Checar logs
- Debug código fonte, parâmetros e configurações
- Documentação
  - Online e offline
- Suporte técnico
- Daemon executando corretamente
- Ordem das coisas
  - Requisitos para funcionamento estão sendo atendidos

# Usando as ferramentas certas

- Já tentou crimpar cabo sem crimpador?
- Saber como a ferramenta funciona, qual o proposito e onde se encaixa no seu cenário.
- Ter as ferramentas básicas sempre a seu alcance.
- Lembre-se: Você é a ponte que conecta a situação ao recurso!



- Físico: Testador de cabos, OTDR, Power Meter
- Tabela ARP: arp
- Coleta pacotes: Wireshark / TCPDump / Kismet
- Conectividade IP: Ping(6) / Traceroute(6) / Tracert
- Configuração placa rede: ifconfig, ip / ipconfig
- DNS: Dig / Nslookup
- Descoberta portas: Netstat (-6), Nmap

- Rotas: route(6) , ip route
- Acesso remoto: Telnet / SSH / Putty
- Gráficos tempo real: Zabbix / Cacti / Icinga / etc
- SNMP: snmpwalk / snmpget
- Ip Calculator: ipcalc
- Qualidade acesso: SIMET / iperf
- Logs: Syslog
- Acesso HTTP(S): Navegadores



- **Looking Glass**
  - PTTs
  - Grandes ASes
- **Alguns abertos**
  - <https://routerproxy.grnoc.iu.edu/internet2/>
  - [lg.ba.ptt.br](http://lg.ba.ptt.br)
  - [lg.sp.ptt.br](http://lg.sp.ptt.br)

- Use boa metodologia
- Documente ações e resultados
- Use ferramentas para colher informações
- Use analisador de protocolo para detalhes do tráfego da rede
- Entender a rede e os protocolos que está fazendo troubleshoot

- **Evitar problemas**
  - BCP38 (Anti-spoofing)
  - Manter sistemas atualizados
  - Backup e versionamento de configurações
  - Redundância de recursos
  - Prefira soluções estáveis e de longo prazo
  - Homologação e prova de conceito (POC)
    - Testes antes de por em funcionamento
    - Modelo prático para provar um conceito ou idéia

- Práticas ITIL
  - Gestão de mudanças

## ^ Campos Personalizados

Resumo: Desativação do serviço NTP nos equipamentos que não estão com os requisitos necessários para tratar o evento de leap second

TipoMudanca: Emergencial

MotivoMudanca: Evento de ajustamento de relógio leap second.

Solicitante: Ibirisol Fontes

Executor: Ibirisol Fontes, Thiago Bomfim

DataAvaliacaoMudanca: (sem valor)

Impacto: Medio

StatusMudanca: Aguardando avaliacao do CM

RiscoEmFazer: Baixo

RiscoEmFazer-Justificativa: Apenas não estaremos com a sincronia fina do NTP, continuaremos com os horários registrados localmente.

RiscoEmNaoFazer: Alto

RiscoEmNaoFazer-Justificativa: Corre-se o risco de serviços que dependam de sincronia de relógio apresentem problema que comprometam o funcionamento ou sejam interrompidos.

IndisponibilidadeDeServicos: Nao

ServicosIndisponibilizados: (sem valor)

TempoIndisponibilidade: (sem valor)

ServicosAfetados: (sem valor)

PessoasNotificadas: (sem valor)

Passo-a-PassoDaMudanca: <https://www.pop-ba.rnp.br/IntranetPOPBA/PP-167>,  
<https://www.pop-ba.rnp.br/IntranetPOPBA/PP-168>

DataHoralInicio: 2015.06.30, 17:00

DataHoraFim: 2015.06.30, 18:00

ResultadoMudanca: Executada com sucesso

Perguntas?

# Atividades Práticas

FORUM  
IX.br - Salvador

28 e 29 de setembro 2017



- Maxham, J. (2014). *The Art Of Troubleshooting*. CreateSpace Independent Publishing Platform.
- RANJBAR, Amir. Troubleshooting and Maintaining Cisco IP Networks (TSHOOT)||. 2010.
- Johnson, Eric. Lane, Peter. 802.11ac Wave 2 Technology Deep Dive and Deployment Recommendations. In: Atmosphere, March. 2015.