



TIC

AULA 06

PROF. ROBERTO

O QUE VAMOS VER NESSA AULA

- Protocolo IPv4:
 - Datagrama
 - TTL
 - Fragmentação e MTU
 - Mensagens de ICMPv4

- Introdução ao Packet Tracer
 - Entendendo o funcionamento;



O QUE VAMOS VER NESSA AULA

■ Configuração básica:

- HUB;
- Switch;
- Roteador;
- DNS;
- DHCP;
- Colocar Banner;
- Colocar Senha;
- Salvar alterações;
- Descrição nas portas;

■ Roteador:

- Alterar nome roteador;





1.

IP V4

Vamos entender o que é o IPv4

IP V4 - O QUE É?



Definição:

- IPv4 é a quarta versão do Protocolo de Internet (IP).
- Utilizado para identificar dispositivos em uma rede por meio de endereços IP.

Estrutura de Endereço IPv4:

- 32 bits divididos em quatro octetos.
- Representado em notação decimal separada por pontos (ex.: 192.168.0.1).

Importância:

- Base da comunicação na Internet e redes locais.

IP V4 - O QUE É?



128	64	32	16	8	4	2	1
-----	----	----	----	---	---	---	---

Valor em Decimal do Bit

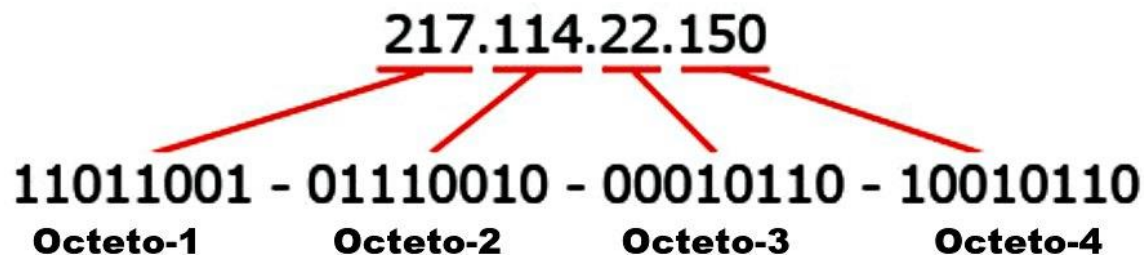
0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1
-----	-----	-----	-----	-----	-----	-----	-----

Valor em Binário

7	6	5	4	3	2	1	0
---	---	---	---	---	---	---	---

Posição do Bit

Byte - Octeto



IP V4 - DATAGRAMA



TIC



INFORMAÇÃO

COMUNICAÇÃO

0

4

8

16

24

31

Versão

Comp.
Cabeçalho

Tipo de Serviço
(TOS)

Comprimento Total

Identificação

Flag

Offset de Fragmento

TTL (Time to Live)

Protocolo

Checksum

Endereço de Origem (32 bits)

Endereço de Destino (32 bits)

Dados

IP V4 - DATAGRAMA



Cabeçalho IPv4

- **Versão:** 4 para IPv4.
- **Comprimento do Cabeçalho:** Tamanho do cabeçalho IP.
- **Tipo de Serviço (ToS):** Qualidade do serviço e prioridade.
- **Comprimento Total:** Tamanho total do datagrama (cabeçalho + dados).
- **Identificação:** Identifica fragmentos do mesmo datagrama.
- **Flags:** Controle de fragmentação.

IP V4 - DATAGRAMA



Cabeçalho IPv4

- Offset de Fragmento: Posição do fragmento dentro do datagrama original.
- TTL (Time To Live): Número de saltos que o pacote pode fazer.
- Protocolo: Protocolo da camada superior (TCP, UDP, ICMP).
- Checksum do Cabeçalho: Verificação de erros no cabeçalho.
- Endereço de Origem: IP de origem.
- Endereço de Destino: IP de destino.

Dados: Informação a ser transmitida.

IP V4 – MTU FRAGMENTAÇÃO



■ MTU (Maximum Transmission Unit):

- O maior tamanho de pacote que pode ser transmitido em um enlace de rede.
- Varia de acordo com o tipo de enlace (ex.: Ethernet normalmente tem MTU de 1500 bytes).

■ Fragmentação:

- Divisão de um datagrama IPv4 em fragmentos menores quando o tamanho do datagrama excede a MTU do enlace.

IP V4 - FRAGMENTAÇÃO E MTU

Transmissor



Dados: 4000
bytes

Fragmentação

MTU do caminho: 1500 bytes

Fragmento 3
1060 bytes

Fragmento 2
1500 bytes

Fragmento 1
1500 bytes

Receptor



Dados: 4000
bytes

Remontagem

Bóson Treinamentos em Tecnologia

IP V4 - MTU FRAGMENTAÇÃO - PROCESSO



Recepção do Datagrama

- Roteador recebe um datagrama maior que a MTU do próximo enlace.

Divisão em Fragmentos

- Datagrama é dividido em fragmentos menores que a MTU.

Adição de Cabeçalhos aos Fragmentos

- Cada fragmento recebe um cabeçalho IPv4 com campos de fragmentação apropriados.

Envio dos Fragmentos

- Fragmentos são enviados individualmente pelo enlace.

Remontagem dos Fragmentos

- Dispositivo de destino recebe os fragmentos e os remonta no datagrama original.

IP V4 - MTU FRAGMENTAÇÃO - IMPACTO



Desempenho:

- A fragmentação pode causar overhead adicional devido à necessidade de processamento extra.

Segurança:

- Fragmentos podem ser usados para ocultar dados maliciosos, dificultando a detecção de ataques.

Confiabilidade:

- A perda de um único fragmento implica a necessidade de retransmitir todo o datagrama.

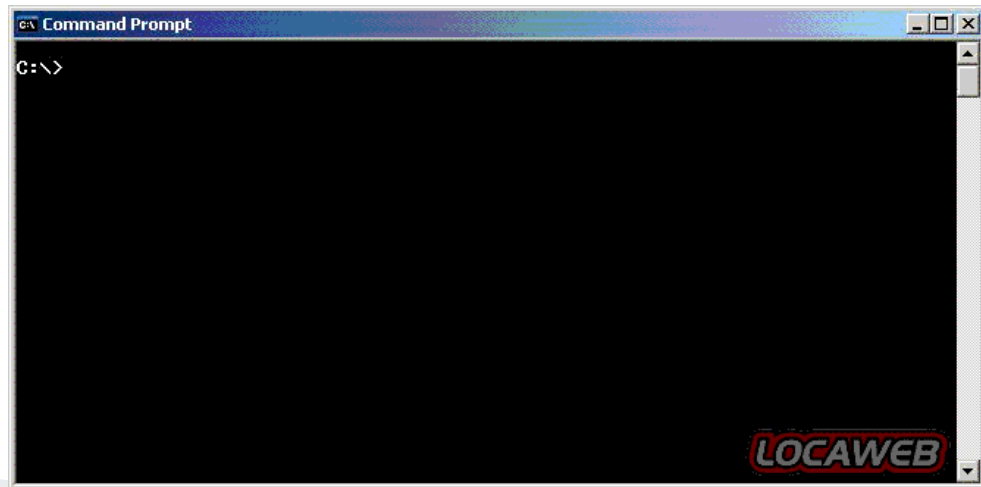
Diagnóstico:

- Ferramentas como Ping e Traceroute podem ser usadas para testar problemas de fragmentação.

IP V4 – MENSAGEM ICMP V4



- Basicamente nos utilizamos o protocolo ICMPv4 para verificar se um host na rede pode ser alcançado.
- É o famoso ping



2.

INTRODUÇÃO PACKET TRACER

Vamos entender o software



PACKET TRACER – O QUE É?



- O que é o Cisco Packet Tracer?
 - Ferramenta de simulação de rede desenvolvida pela Cisco:
 - ▶ Permite a criação e simulação de redes virtuais;
 - ▶ Utilizado amplamente em ambientes educacionais e por profissionais de redes;

PACKET TRACER – O QUE É?



- O que é o Cisco Packet Tracer?
 - Utilizada para ensino e aprendizado de redes:
 - ▶ Ferramenta essencial para cursos de redes, como o Cisco Networking Academy
 - ▶ Ajuda a compreender conceitos de redes de forma prática e visual

PACKET TRACER – O QUE É?



- O que é o Cisco Packet Tracer?
 - Disponível para estudantes e profissionais:
 - ▶ Versões para Windows, Linux, macOS e dispositivos móveis
 - ▶ Gratuita para estudantes, professores e profissionais da área de redes

PACKET TRACER – CARACTERÍSTICAS



■ **Simulação de Redes Complexas:**

- Capacidade de criar redes que variam de simples a extremamente complexas
- Simulação de topologias de rede de pequeno, médio e grande porte

PACKET TRACER – CARACTERÍSTICAS



■ Suporte a uma Ampla Gama de Dispositivos de Rede:

- Roteadores, switches, firewalls, pontos de acesso, etc.
- Dispositivos Cisco e genéricos para simulações realistas.

■ Ambiente de Simulação Interativo:

- Interface gráfica amigável e intuitiva
- Arrastar e soltar para adicionar e conectar dispositivos

PACKET TRACER – CARACTERÍSTICAS



Ferramentas de Análise de Pacotes:

- Captura de pacotes em tempo real
- Visualização detalhada dos headers de pacotes e dados transmitidos;

Integração com Programas de Certificação Cisco:

- Alinhado com os currículos de certificação Cisco (CCNA, CCNP, etc.)
- Atividades e laboratórios práticos baseados em cenários de certificação

PACKET TRACER – BENEFÍCIOS



- Aprendizado prático sem necessidade de hardware físico.

- Desenvolvimento de habilidades de troubleshooting.

- Visualização e compreensão de protocolos de rede.

- Preparação para exames de certificação Cisco.



2.

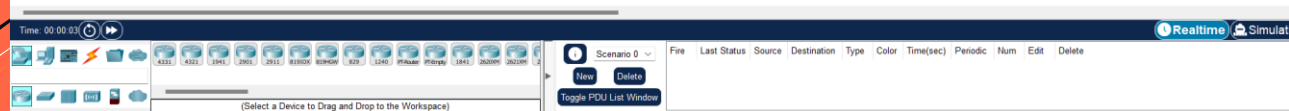
UTILIZANDO O SIMULADOR

Vamos criar e testar os primeiros cenários.

PACKET TRACER



Ao abrir o software vai aparecer a seguinte tela.

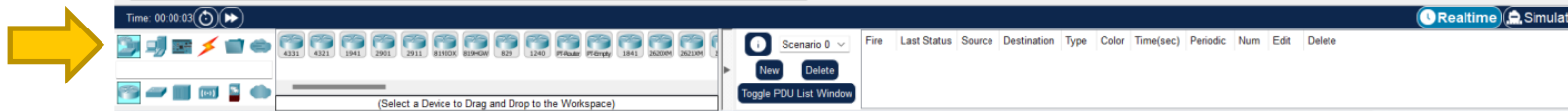




Área de trabalho



Equipamentos



Real time

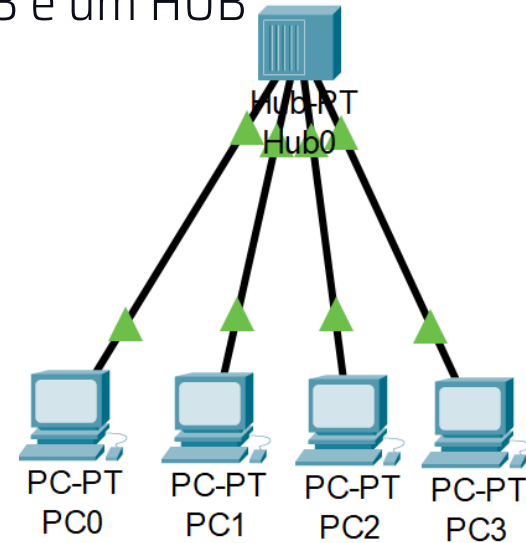


simulador

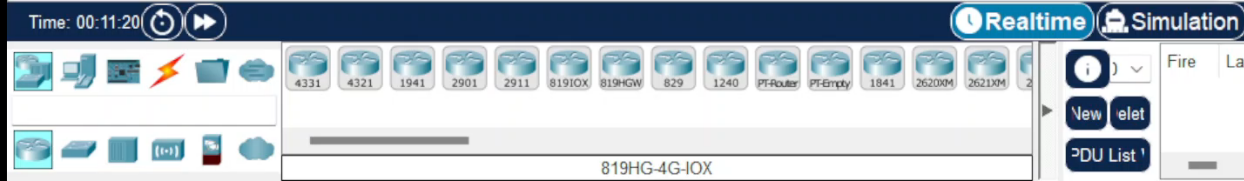
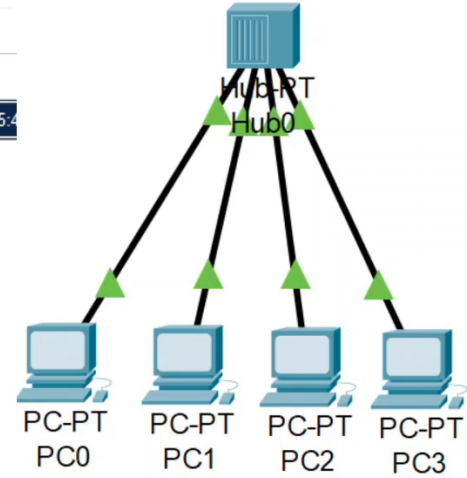
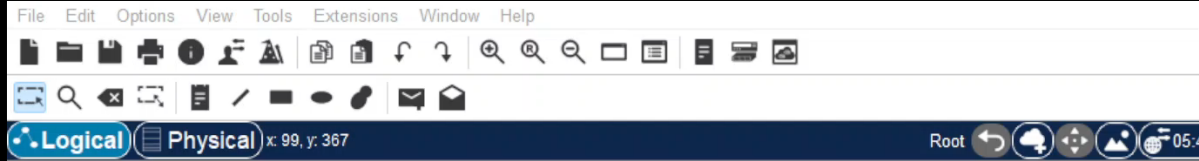
PACKET TRACER – 1º CENÁRIO



Vamos testar o funcionamento do HUB, para isso vamos criar um cenário com 4 computadores IP's fixo 192.168.0.10, 11, 12 e 13 e um HUB



VÍDEO - O AUTOR



PACKET TRACER - 2º CENÁRIO



TECNOLOGIA

TIC

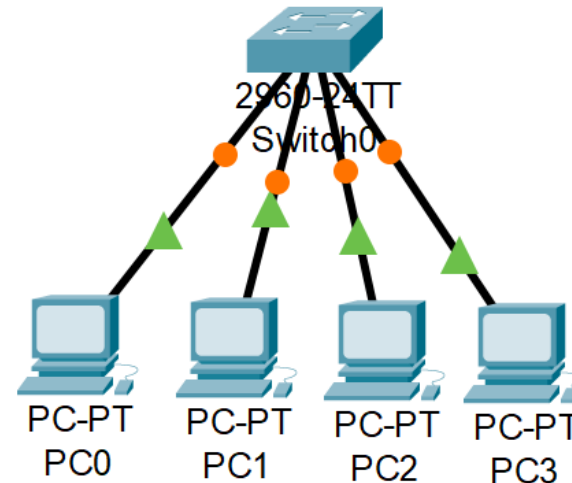


INFORMAÇÃO



COMUNICAÇÃO

Vamos testar o funcionamento do switch, para isso vamos criar um cenário com 4 computadores IP's fixo 192.168.0.10, 11, 12 e 13 e um switch



VÍDEO - O AUTOR

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.11

Pinging 192.168.0.11 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.0.11

Pinging 192.168.0.11 with 32 bytes of data:
Reply from 192.168.0.11: bytes=32 time=1ms TTL=128
Reply from 192.168.0.11: bytes=32 time=1ms TTL=128
Reply from 192.168.0.11: bytes=32 time=1ms TTL=128
Reply from 192.168.0.11: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 1ms
C:\>ping 192.168.0.11

Pinging 192.168.0.11 with 32 bytes of data:
```

Root 14:18:30

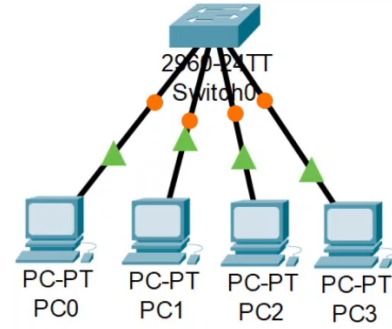
Time: 00:27:08

Realtime Simulation

View Reset

DU List

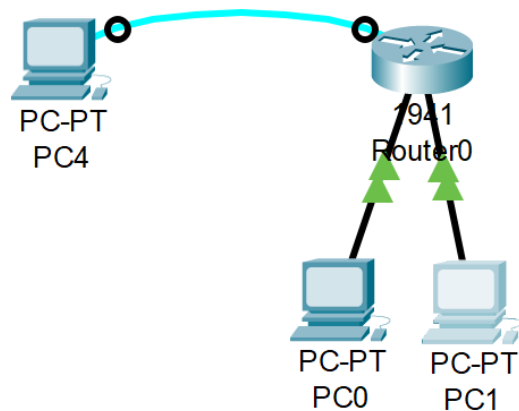
Copper Straight-Through



PACKET TRACER – 3º CENÁRIO



Vamos testar o funcionamento do roteador, para isso vamos criar um cenário com 2 computadores IP's fixo 192.168.0.10 o outro com ip 192.168.1.10 e 1 roteador, com um computador com cabo console para configurarmos o roteador



VÍDEO - O AUTOR

The screenshot displays the Cisco Packet Tracer application window. The top menu bar includes File, Edit, Options, View, Tools, Extensions, Window, and Help. Below the menu is a toolbar with various icons for creating and editing network components. The main workspace is divided into two tabs: 'Logical' (selected) and 'Physical'. The 'Logical' tab shows a network diagram with a central router labeled 'Router0' and three PCs labeled 'PC-PT PC0', 'PC-PT PC1', and 'PC-PT PC4'. The router is connected to PC0 and PC1, and PC4 is connected to the router via a cloud. The 'Physical' tab shows a detailed view of the selected component, currently displaying 'x 29, y: 405'. On the right side, there is a 'Simulation' panel with a 'Reset Simulation' button, a 'Constant Delay' checkbox (checked), and a 'Captured to:' field (no captures). Below this is a 'Play Controls' section with play, pause, and stop buttons. Further down is an 'Event List Filters - Visible Events' section listing various network protocols and services. At the bottom, there is a 'Time: 00:30:54.095' display, a 'PLAY CONTROLS' section with play, pause, and stop buttons, and a 'Simulation' panel with 'Event List', 'Realtime', and 'Simulation' tabs. The 'Simulation' tab is selected, showing a 'Fire' button and a 'La' button. The bottom status bar indicates 'Automatically Choose Connection Type'.

File Edit Options View Tools Extensions Window Help

Logical Physical x 29, y: 405

Simulation

Event List

Vis. Time(sec) Last Device

Reset Simulation ☒ Constant Delay Captured to: (no captures)

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters Show All/None

Time: 00:30:54.095 PLAY CONTROLS

Event List Realtime Simulation

Fire La

New delet

DU List

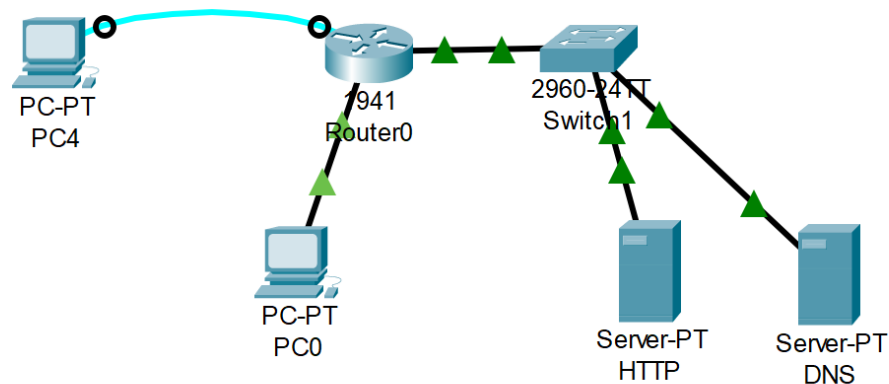
Automatically Choose Connection Type

PACKET TRACER – 4º CENÁRIO



Agora vamos atualizar o que foi feito com o roteador, vamos colocar um switch e 2 servidores 1 de DNS e um HTTP.

A ideia é criarmos o site www.teste.com.br. Para acessar a página não podemos digitar o IP do servidor HTTP.



PACKET TRACER – 5º CENÁRIO

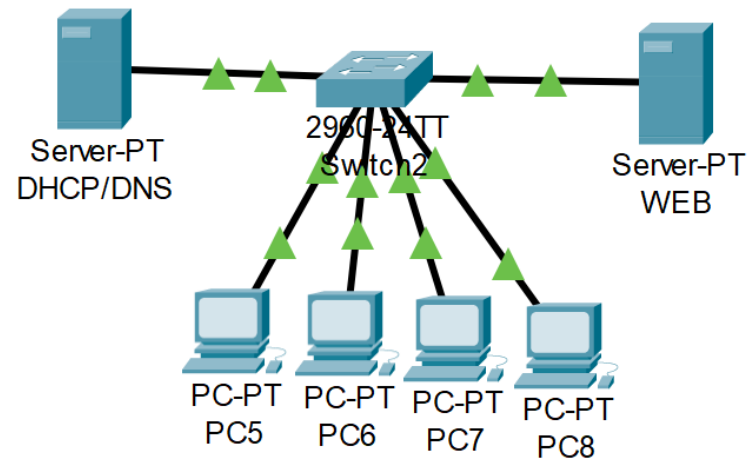


Vamos começar a ampliar a rede, nesse cenário vamos ter 4 computadores, 1 switch e 2 servidores, 1 servidor DHCP e DNS e outro de WEB.

Devemos configurar o DHCP para distribuir IP a partir do IP 192.168.1.20 máscara padrão.

Servidor DNS/DHCP IP: 192.168.1.2

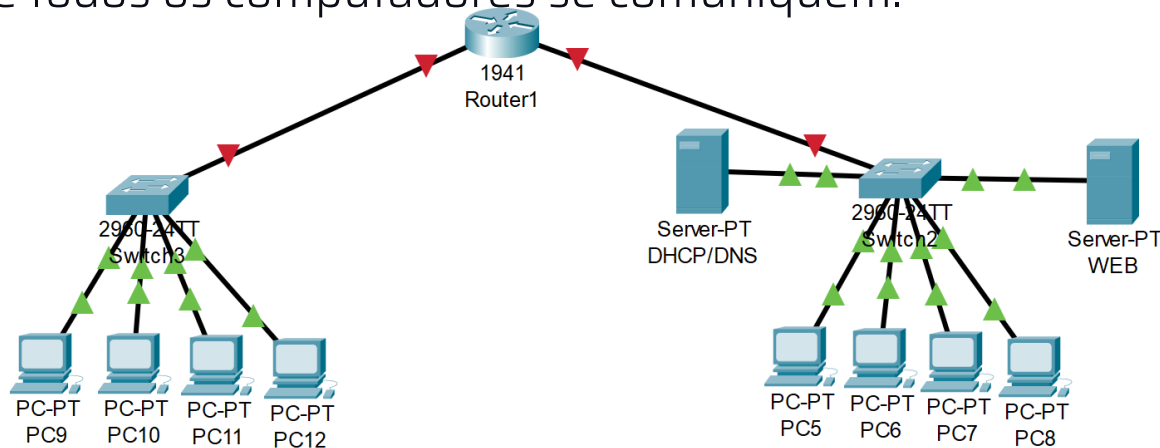
Servidor WEB: 192.168.1.3



PACKET TRACER – 6º CENÁRIO



Estruturar a rede para que todos os computadores se comuniquem.



ROTEADOR - HOSTNAME



- Quando iniciamos a configuração de um roteador devemos fazer algumas configurações básicas, como alterar o nome do dispositivo.
- Por padrão todo roteador quando ligamos ele vem com o nome “route”
- Vamos alterar esse nome para qualquer outro por exemplo.
- **Router#hostname Teste123**

ROTEADOR - HOSTNAME



- Caso apresente erro temos que acessar a configuração do roteador para isso temos que digitar:
- enable
- configure terminal
- Depois podemos digitar hostname Teste123

ROTEADOR - BANNER



- Também é bem vindo colocarmos um banner de boas vindas quando acessamos um roteador

```
Telnet 10.1.1.2

User Access Verification

Password:
*****
*****
****
****
****
      YOU HAVE SUCCESSFULLY ENTERED THIS SYSTEM
RTR20 on line 130. BE ADVISED YOUR
ACTIONS ARE LOGGED AND AUDITS ARE PERFORMED
DAILY. IF YOU HAVE ANY QUESTIONS CONTACT THE
SYSTEM ADMINISTRATOR AT 555-5555, EMAIL AT
WILECOYOTE@ACMECORP.NET.
****
****
      THANK YOU
****
****
      WIL E. COYOTE
      NETWORK ADMINISTRATOR
****
****
*****
*****
```

ROTEADOR - BANNER



- Para colocarmos o banner é bem simples, no terminal digite.
- **enable**
- **configure terminal**
- **banner motd # Acesso não permitido! #**
- Temos a configuração do banner na tela de login, para isso so alterar o motd para login

ROTEADOR - SENHA



- É necessário colocarmos uma senha no roteador, para poder acessar, caso contrário qualquer pessoa vai acessar. Para isso no terminal digite.
- **enable**
- **conf t**
- **enable secret senai123** → Colocamos a senha senai123
- **line console 0** → Acessa o console 0
- **password senai123** → define senha senai123 no console
- **Login** → habilita que login no consele
- **Exit** → sai da configuração
- **Logout** → faz logoff

ROTEADOR - SENHA



TECNOLOGIA

TIC



INFORMAÇÃO



COMUNICAÇÃO

- line vty 0 4 → configura acesso remote do 0 ao terminal 4
- password senai123 → senha
- Login → Exige login
- *Depois vamos criptografar nossas senhas que foram em texto puro*
- exit
- service password-encryption
- Senha configurada.

ROTEADOR - COLOCAR DESCRIÇÃO NA PORTA



■ É muito comum colocarmos uma descrição na porta do roteador para sabermos onde vai o link de conexão, para isso devemos, acessar a interface de rede e depois:

■ **description Link to LAN 1**

■ Pronto bem simples, essas são as primeiras configurações vamos fazer alguns exercícios

ROTEADOR - SALVAR



- Como sabemos temos que salvar tudo que fazemos para isso o comando é simples:
- Devemos sair da configuração global para podermos fazer a gravação.
- Digite: **copy running-config startup-config**
- Ou apenas
- **wr**

OBRIGADO!

