

Engenharia de Computação

Redes de Computadores

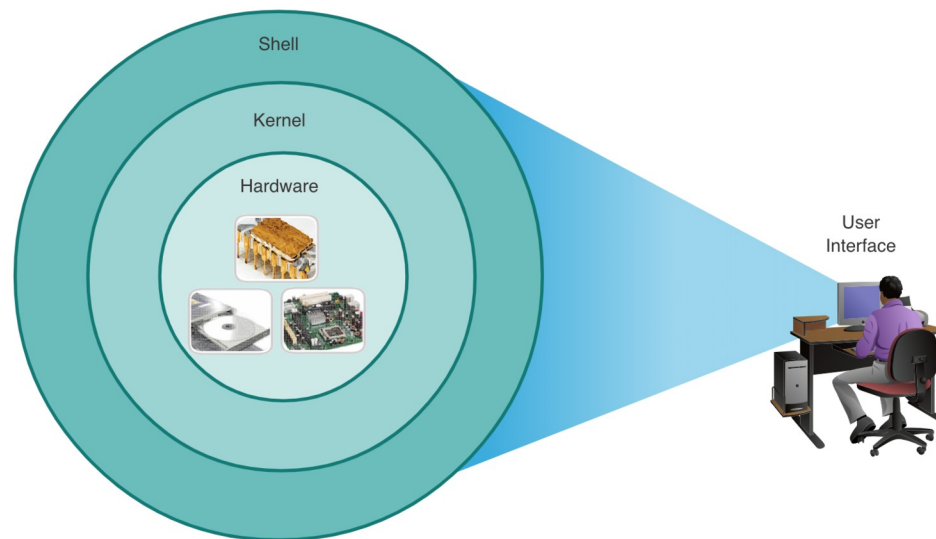
Aula IOS - Cisco

Prof. Fernando Barreto

informatica-ap@utfpr.edu.br

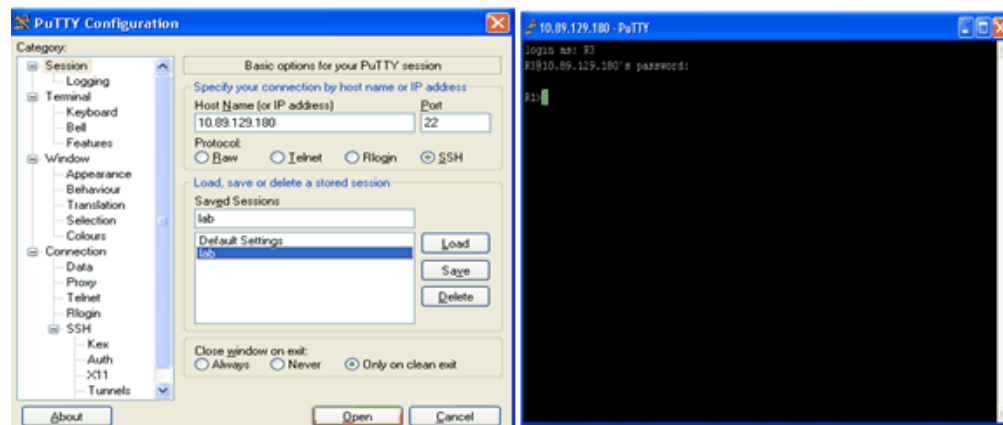
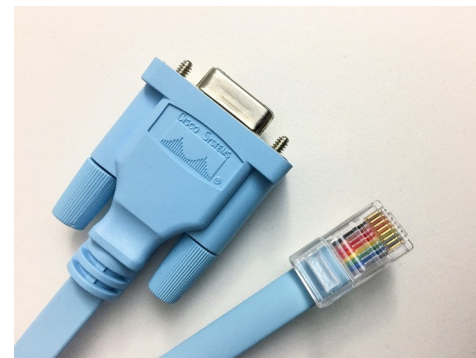
Laboratório: Comandos no Packet Tracer

- **Shell** - A interface de usuário que permite que os usuários solicitem tarefas específicas do computador. Essas solicitações podem ser feitas por meio da interface (Command Line Internet) CLI ou (Graphical User Interface) GUI.
- **Kernel** - comunica-se entre o hardware e o software de um computador e gerencia como os recursos de hardware são usados para atender aos requisitos de software.
- **Hardware** - A parte física de um computador, incluindo os componentes eletrônicos subjacentes.



Cisco Internet Operating System (IOS)

- **Console** — Uma porta de gerenciamento física usada para acessar um dispositivo para fornecer manutenção, como executar as configurações iniciais.
- **Shell segura (SSH)** – Estabelece uma conexão CLI segura remota com um dispositivo, por meio de uma interface virtual, em uma rede. (Nota: Este é o método recomendado para se conectar remotamente a um dispositivo.)
- **Telnet** — Estabelece uma conexão CLI remota insegura a um dispositivo através da rede. (Nota: a autenticação do usuário, senhas e comandos são enviados pela rede em texto sem formatação.)



Modo EXEC do Usuário

- Permite acesso a apenas um número limitado de comandos básicos de monitoramento
- Identificado pelo prompt da CLI que termina com o símbolo >

```
Router>
```

```
Switch>
```

Modo EXEC com privilégios:

- Permite acesso a todos os comandos e recursos
- Identificado pelo prompt da CLI que termina com o símbolo #

```
Router#
```

```
Switch#
```

Mudar para Modo EXEC com privilégios:

- Para passar do modo EXEC usuário para o modo EXEC privilegiado, use o comando **enable**.
- Para sair do modo EXEC privilegiado e volta ao modo EXEC usuário: **disable**

```
Switch> enable  
Switch#
```

Modo de configuração global

- Usado para acessar opções de configuração no dispositivo quando no modo EXEC privilegiado: **configure terminal** . Para sair, **exit**

```
Switch(config)#  
Switch(config)#exit  
Switch#
```

Modo de configuração de linhas

- Usado no modo configuração para configurar o acesso ao Console, SSH, Telnet ou AUX.
Exemplo: **line console 0**

```
Switch(config-line)#
```

Modo de configuração de interface

- Usado no modo configuração para configurar uma porta de switch ou interface de roteador.
Exemplo: **interface fastethernet 0/0**

```
Switch(config-if)#
```

▪ Modo de configuração global

- Para entrar e sair do modo de configuração global, use o comando **configure terminal**. Retorne ao modo EXEC privilegiado com o comando **exit**.

```
Switch(config)#
Switch(config)#exit
Switch#
```

▪ Modo de configuração de linhas

- Para entrar e sair do modo de configuração de linha, use o comando de **line** seguido pelo tipo de linha de gerenciamento. Retorne ao modo de configuração global usando o comando **exit**. Com o comando **end**, ou teclas **Ctrl +Z**, retorna direto ao modo EXEC privilegiado.

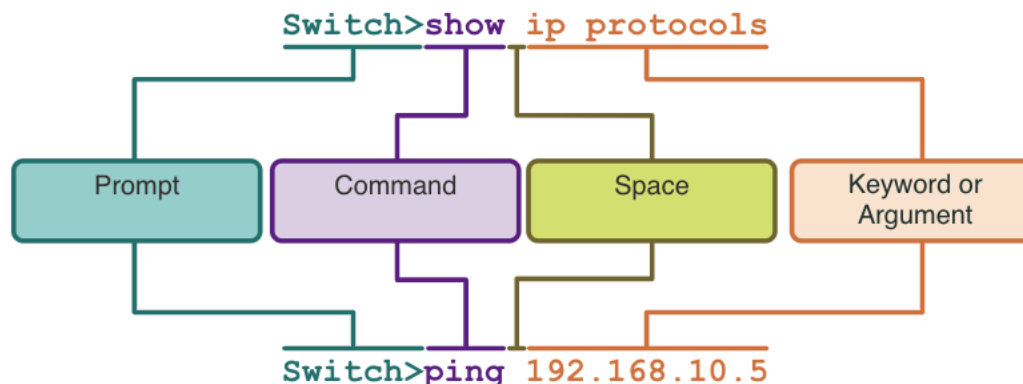
```
Switch(config)#line console 0
Switch(config-line)#exit
Switch(config)#
```

```
Switch(config)#line console 0
Switch(config-line)#end
Switch#
```

Modos de subconfiguração:

- Para mover diretamente de um modo de subconfiguração para outro, digite o comando de modo de subconfiguração desejado. No exemplo, o prompt de comando muda de **(config-line)#** para **(config-if)#**.

```
Switch(config-line)#interface FastEthernet 0/1
Switch(config-if)#
```



- **Palavra-chave** - este é um parâmetro específico definido no sistema operacional (na figura, ip protocols)
- **Argumento** - não predefinido; um valor ou variável definido pelo usuário (na figura, 192.168.10.5)
- Uso do ?
 - Ex: ? ou confi? ou configure ?
- Abreviaturas: Exemplo, no modo exec privilegiado, conf é único para configure
- Uso da tecla **tab**: autocompleta ou opções

- Backspace: Apaga caracter do comando
- Enter: Mostra a próxima linha quando apresentado a tela "---More---"
- Barra de espaço: Mostra a próxima tela quando apresentado "---More---"
- Ctrl-C ou Ctrl-Z: Quando no modo config, termina o modo config e retornar ao modo EXEC privilegiado
- Setas:
 - ↑ e ↓: navegar no histórico de comandos
 - → e ←: navegar nos caracteres do comando atual em edição
- Ctrl-Shift-6: Encerra comando/sequência de programas. Ex: interromper consulta DNS, traces, pings, etc.

Mais informações:

<https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-0/command/reference/cli70bk/cli70over.pdf>

<https://ldapwiki.com/wiki/CISCO%20Commands>

- Diretriz para dispositivos de nomeação:
 - Começar com letra
 - Somente pode conter letras, números e traços
 - Não deve conter espaços
 - Terminar com letra ou número
 - Máximo de 64 caracteres
- Comando no modo config:
 - **hostname** nome_do_dispositivo

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

Nota: Para retornar o switch ao prompt padrão, use o comando **no hostname** global config.



- **Diretrizes de senha**

- Usar senhas com mais de oito caracteres.
 - **security passwords min-length tam**
(obs: depende do suporte do IOS)
- Use uma combinação de letras maiúsculas e minúsculas, números, caracteres especiais e/ou sequências numéricas.
- Evite usar a mesma senha para todos os dispositivos.

Observação: **a maioria dos laboratórios neste curso usa senhas simples, como cisco ou class.** Essas senhas são consideradas fracas e facilmente adivinháveis e devem ser evitadas nos ambientes de produção.

- **Difícultar ataque de adivinhação**

- **login block-for xx attempts yy within zz**
(obs: depende do suporte do IOS)
 - Bloqueia por xx segundos, se yy tentativas erradas dentro de zz segundos

- **Os dispositivos de rede devem limitar o acesso protegendo:**

- **EXEC de usuário:** Console, login Telnet, login SSH (preferível)
- **EXEC privilegiado:** enable
- Todas as **senhas devem ser criptografadas e notificações legais fornecidas.**

- EXEC usuário (acesso console)

- Primeiro, entre no modo de configuração do console de linha usando o **comando line console 0** no modo de configuração global.
- Em seguida, especifique a senha do modo EXEC usuário com o comando:

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

- **password** *senha*

- Por fim, use o comando **login** para permitir o acesso ao EXEC usuário
- Pode-se definir tempo ocioso de exec
 - **exec-timeout** *xx yy* (xx min, yy seg)

- EXEC privilegiado

- Primeiro entre no modo de configuração global. Em seguida, use o comando:

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

- **enable secret** *senha*

- **OBS**: comando enable password *senha* deixa em texto puro no arquivo de configuração, sendo pouco usado

- EXEC usuário (acesso vty - telnet)

- Primeiro entre no modo de configuração VTY de linha usando o comando **line vty 0 15** no modo de configuração global.
- Em seguida, especifique a senha VTY com o comando
 - **password** *senha*
- Por fim, use o comando **login** para permitir o acesso via VTY
- Pode-se definir tempo ocioso de exec (automaticamente faz logout...)
 - **exec-timeout** *xx yy* (xx min, yy seg)

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

OBS: As linhas VTY permitem acesso remoto usando Telnet ou SSH ao dispositivo. Muitos switches Cisco são compatíveis com até 5 linhas VTY (numeradas de 0 a 4) e os mais recentes até 16 linhas VTY (numeradas de 0 a 15).

- EXEC usuário (acesso vty – ssh)
 - Criar chave RSA, usuário e senha para logar por SSH
 - No exemplo abaixo, define-se o domainname , uma chave RSA 1024bits, usuário Bob com senha cisco, e indica o acesso VTY por ssh (não mais telnet) e processo de login com usuários locais

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# ip domain name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com % The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)# username Bob secret cisco
R1(config)# line vty 0 15
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
R1(config)#
```

- Pode-se definir o uso de SSHv2: **ip ssh version 2**
- Pode-se definir também o tempo ocioso de modo privilegiado
 - **exec-timeout** xx yy (xx min, yy seg)

- Os arquivos **startup-config** e **running-config** exibem a maioria das senhas em texto simples.
- Para criptografar senhas: **service password-encryption**.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

- Use o comando **show running-config** para verificar se as senhas do dispositivo agora estão criptografadas.

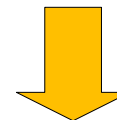
```
Sw-Floor-1# show running-config
!
!
line con 0
password 7 094F471A1A0A
login
!
Line vty 0 4
Password 7 03095A0F034F38435B49150A1819
Login
!
!
end
```

- Uma mensagem de banner é importante para avisar as pessoas não autorizadas que tentarem acessar o dispositivo... (questões legais...)
- Para criar uma mensagem de banner do dia em um dispositivo de rede, use o comando de configuração global:
- **banner motd # *A mensagem ...* #**

OBS: O “#” na sintaxe do comando é denominado caracter de delimitação. Ele é inserido antes e depois da mensagem.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #Authorized Access Only!#
```

O banner será exibido nas tentativas de acessar o dispositivo.



```
Press RETURN to get started.
```

```
Authorized Access Only!
```

```
User Access Verification
```

```
Password:
```

Para acessar o switch remotamente, um endereço IP e uma máscara de sub-rede devem ser configurados na SVI, que é a VLAN 1 de gerência.

Para configurar um SVI em um switch:

- Digite o comando **interface vlan 1** no modo de configuração global.
- Em seguida, atribua um endereço IPv4 adequado usando o comando **ip address** *ip-address subnet-mask*.
- Por fim, ative a interface virtual com o comando de configuração de interface **no shutdown**
 - Por padrão, as interfaces inicialmente ficam em shutdown

- Há dois arquivos de sistema que com a configuração do dispositivo:
 - **startup-config** - Este é o arquivo de configuração salvo armazenado na NVRAM. Ele contém todos os comandos que serão usados pelo dispositivo na inicialização ou reinicialização. O flash não perde seu conteúdo quando o dispositivo está desligado.
 - **running-config** - Isto é armazenado na memória de acesso aleatório (RAM). Ele reflete a configuração atual. A modificação de uma configuração ativa afeta o funcionamento de um dispositivo Cisco imediatamente. Ela perde todo o seu conteúdo quando o dispositivo é desligado ou reiniciado.
 - Para salvar as alterações feitas na configuração de inicialização: **copy running-config startup-config** ou **write**
 - Para ver as configurações, no modo EXEC privilegiado:
 - **show running-config** e **show startup-config**
 - Para reiniciar dispositivo: **reload**
 - Para apagar arquivo de inicialização: **erase startup-config**