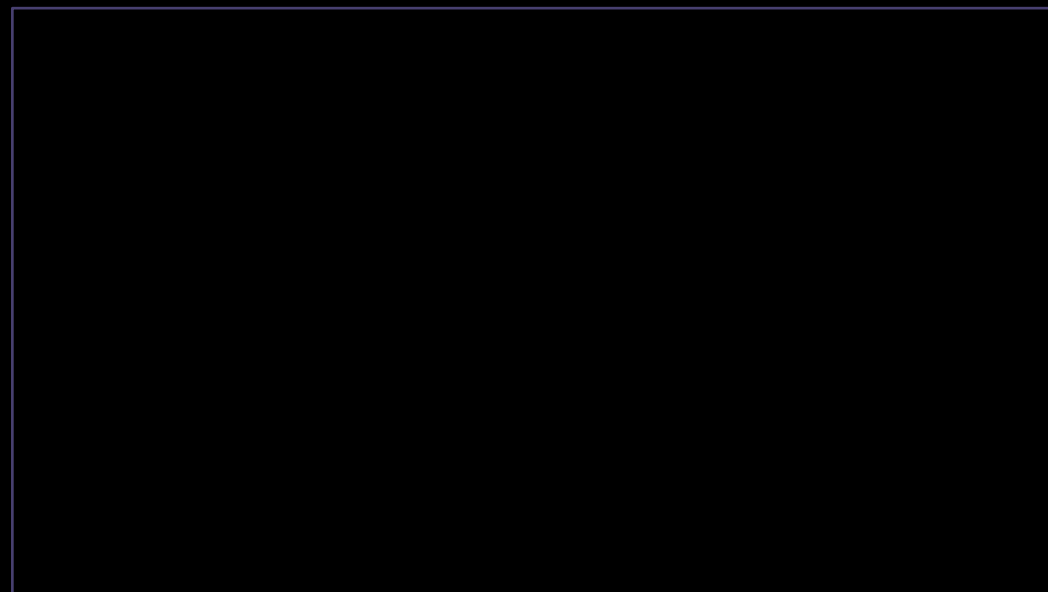




Prime

CCS-A

Protocolos de Camada de
Aplicativo e Práticas Recomendadas
de Segurança de Rede



HTTP e HTTPS

HTTP – Permite que os clientes solicitem páginas da Web de servidores Web e interação com esses mesmos servidores.

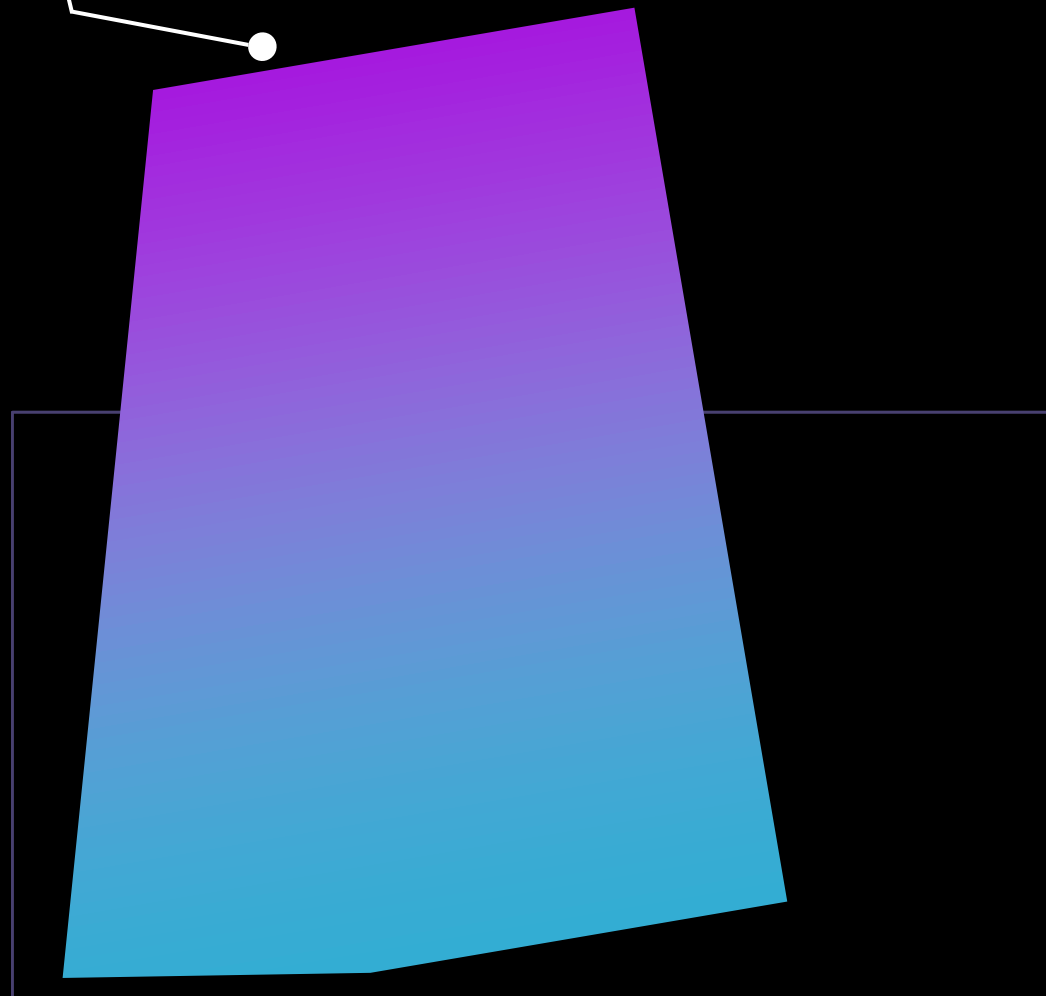
HTTPS – Recebe e envia conteúdo em um formato criptografado com SSL.

- ▶ O endereço começa com **https://**
- ▶ Cadeado fechado ou bloqueado.

DNS



- ▶ Usado para converter nomes de domínio totalmente qualificados em endereços IP.
- ▶ Seu sistema consulta um servidor DNS quando você tenta uma conexão.
- ▶ Se seu sistema tiver o endereço IP do sistema de destino, a conexão com esse sistema será feita.



SMTP



- ▶ Usado para enviar ou rotear mensagens em uma rede TCP/IP.
- ▶ A maioria dos produtos de servidor de e-mail suporta SMTP.

POP3

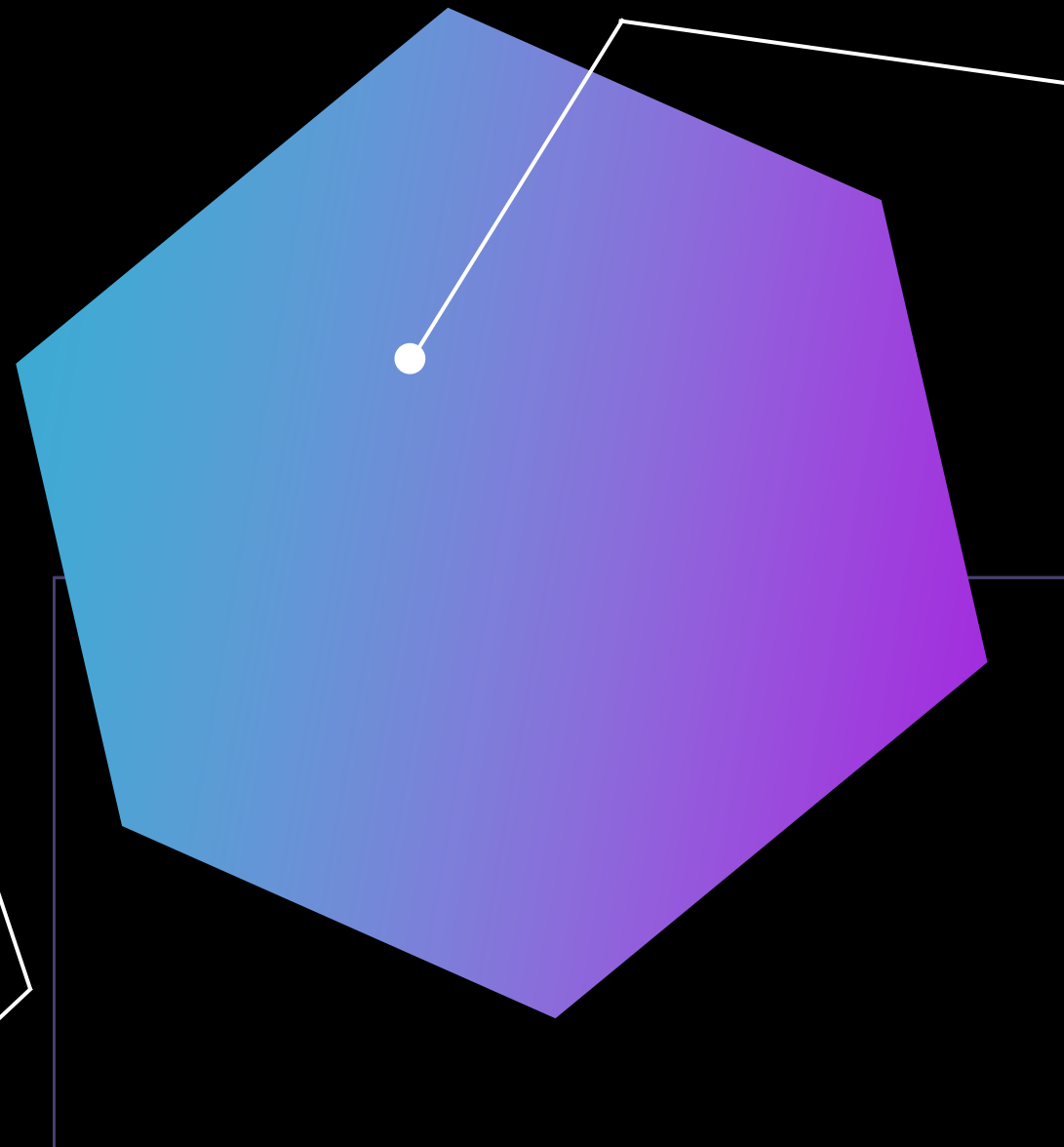
- ▶ Protocolo de Internet usado para recuperar (baixar) e-mail de um servidor de e-mail para o cliente POP3 pela porta TCP 110.
- ▶ O POP3 tem recursos limitados no suporte a pastas.
- ▶ Um cliente POP3 suporta apenas uma caixa de entrada.
- ▶ Se for necessário suporte adicional a pastas, você precisará usar um cliente IMAP4.

IMAP4

- ▶ Protocolo semelhante ao POP3.
- ▶ Permissão para recuperar mensagens de um servidor usando a porta TCP 143.
- ▶ Permite pastas adicionais.



Exemplo: Conexão de pastas públicas armazenadas em um Microsoft Exchange Server.



SNMP

— Padrão da Internet que possibilita gerenciar de forma remota quase todo dispositivo de rede que suporte SNMP.



Placa de rede;



Programa ou serviço;



Hub;



Switch;



Roteador.

SNMP

— **Abordagem de duas camadas:** Sistema de gerenciamento central e a Base de Informações de Gerenciamento (MIB).

— Um sistema de gerenciamento centralizado deve ser capaz de coletar e analisar muitos dados, incluindo:



Identificação e estatísticas do protocolo de rede;



Identificação dinâmica de computadores conectados à rede (referido como descoberta);



Dados de configuração de hardware e software;



Estatísticas de desempenho e uso do computador;



Evento do computador e mensagens de erro;

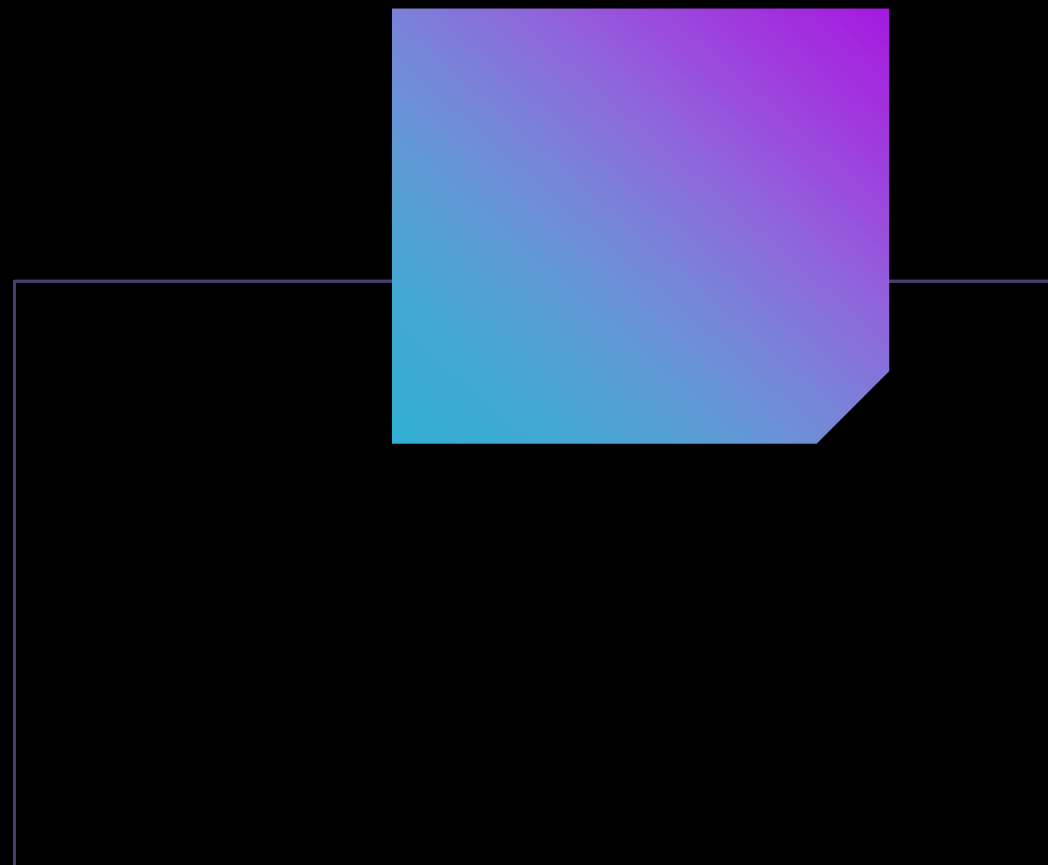


Estatísticas de uso de programas e aplicativos.

FTP

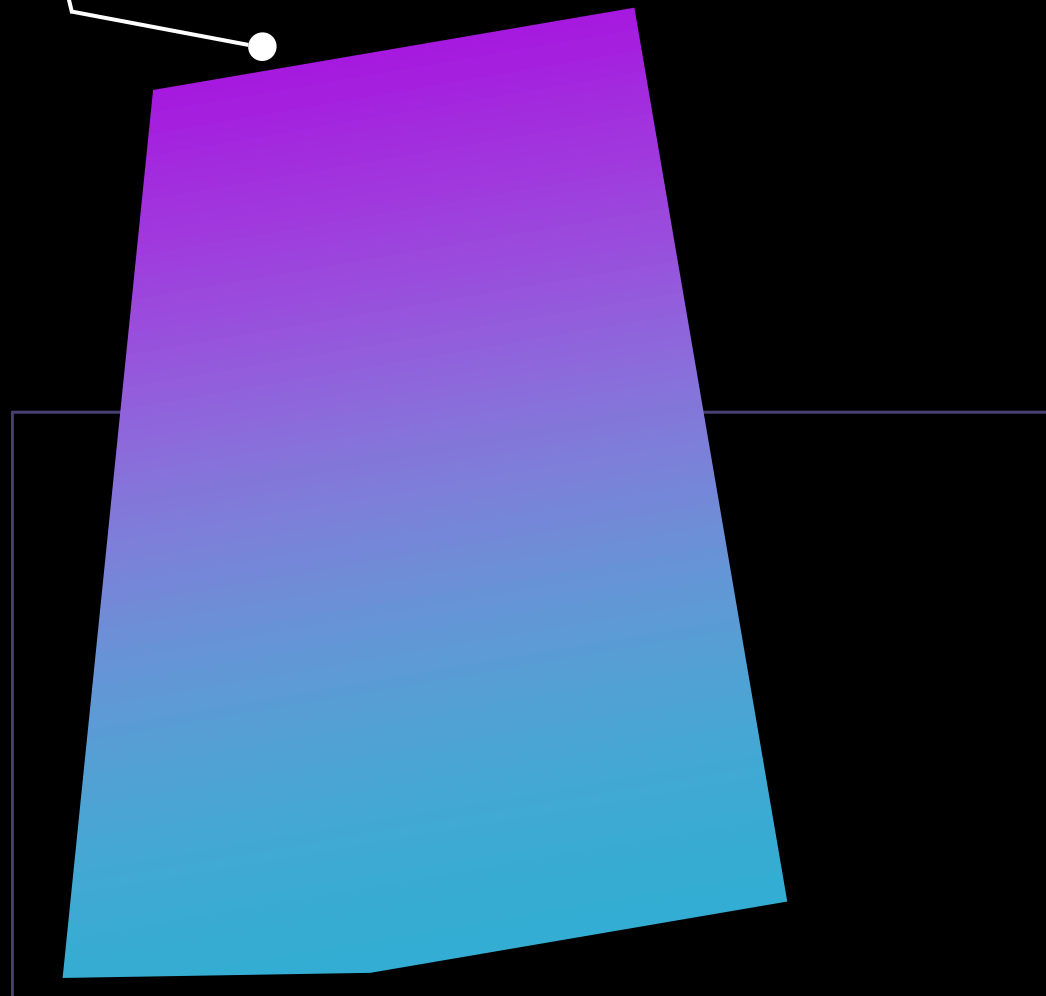


- ▶ Upload e download de arquivos entre servidores e clientes FTP.
- ▶ O FTP estabelece uma conexão com um computador remoto usando o nome do host ou o endereço IP.
- ▶ Instalação do TCP/IP = Utilitário FTP (Sem GUI).
- ▶ Disponível para qualquer sistema operacional.



TFTP

- ▶ Protocolo mais simples que o FTP.
- ▶ Suporta leitura e gravação em arquivos.
- ▶ Normalmente usado para copiar a configuração do roteador e do switch do dispositivo para o servidor TFTP.
- ▶ Inicialização de dispositivo carregando a configuração armazenada em um servidor TFTP.



SFTP

- Criptografa todo o tráfego entre o cliente SFTP e o servidor SFTP.
- Suporte a autenticação de chave pública e compactação de dados;
- Ao contrário do TFTP, suporta diversos comandos.



Lista conteúdo do diretório;



Cria diretório;



Download de arquivos;



Faz upload de arquivos.

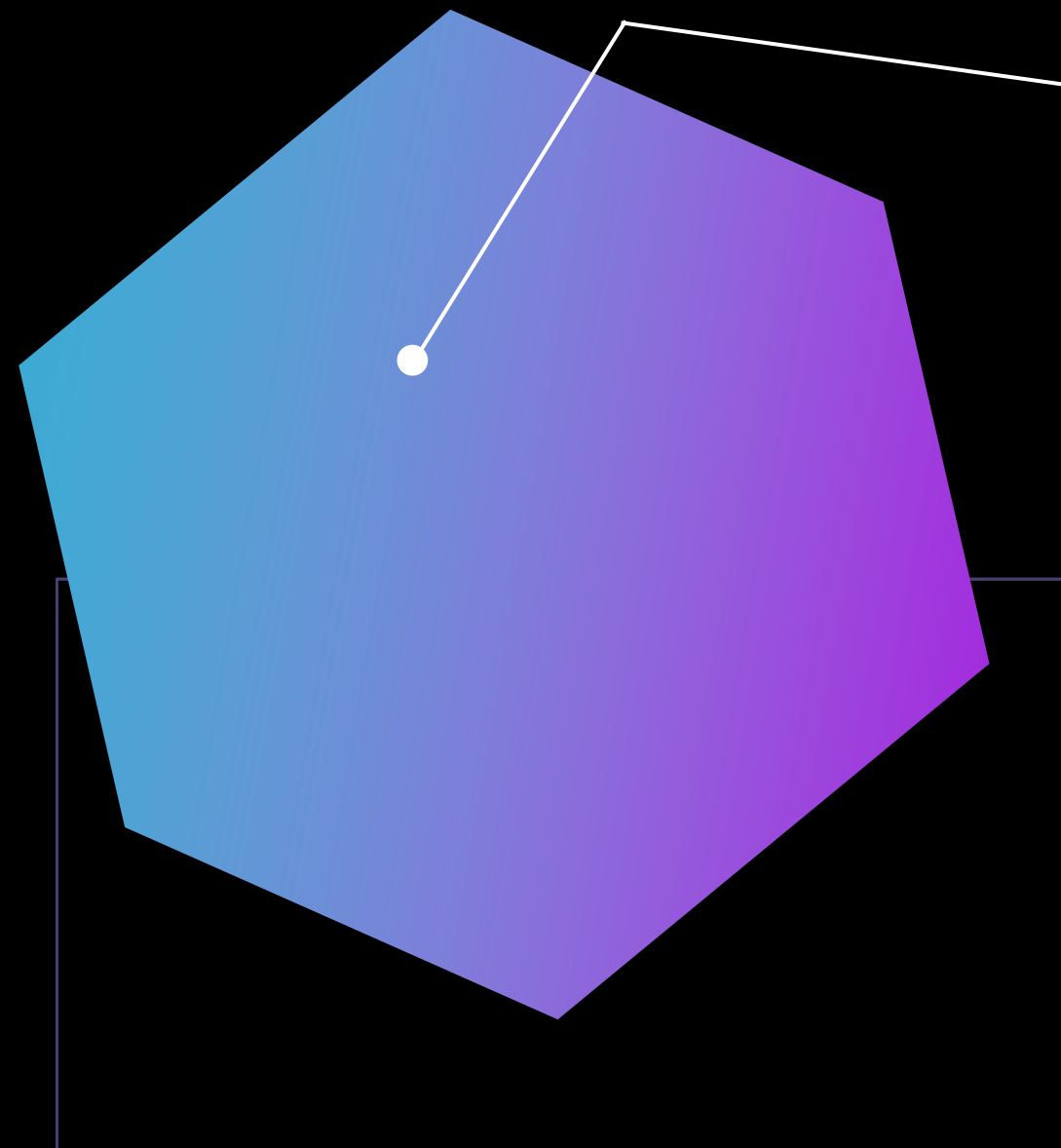
Telnet

- Protocolo de emulação de terminal que permite a execução ou emulação de um programa no servidor.
- Vários dispositivos permitem essa função.
- Utiliza o conjunto de comandos já disponível para uma sessão Telnet (close, display, logout, open, quit, set etc.).

SSH

>—
SSH

- ▶ Criação de shell com um sistema remoto usando uma conexão segura.
- ▶ Pode executar comandos no shell e copiar arquivos para o sistema local.
- ▶ Oferece suporte a shells remotos (ponte entre usuário e servidor).
- ▶ Deve ser usado no lugar do Telnet.

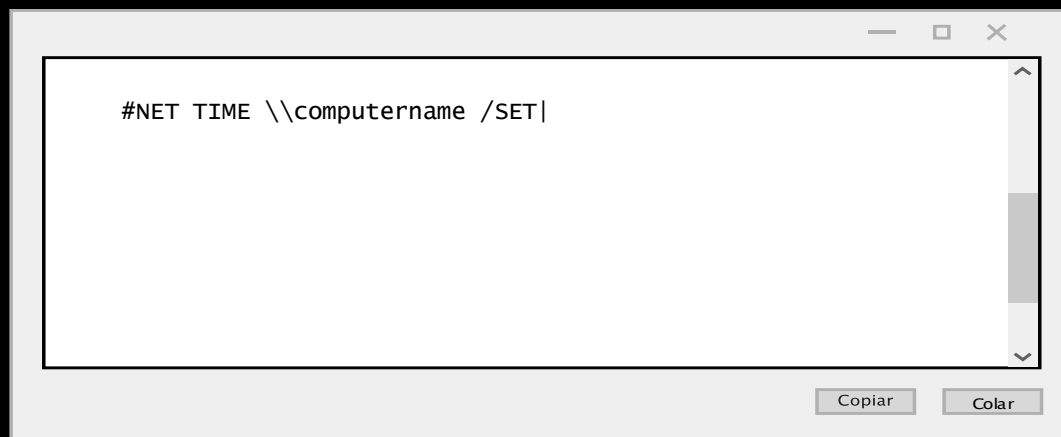


SCP

- ▶ Responsável por copiar arquivos de um servidor remoto para o sistema local.
- ▶ Garante que os dados em trânsito sejam mantidos em sigilo.
- ▶ Usam uma conexão SSH, com usuário e senha.

NTP

- ▶ Sincroniza relógios dos PCs em uma rede.
- ▶ Configuração do servidor, tornando o mesmo um servidor de horário.
- ▶ Para gerenciar, use o comando:



```
#NET TIME \\computernome /SET|
```

- ▶ Emulador PDC (Controlador de Domínio Primário).
- ▶ Sincronização de horário leva em consideração as configurações de fuso horário do seu sistema operacional.



LDAP

- ▶ Protocolo TCP/IP para acesso ao serviço de diretório.
- ▶ Permite que clientes LDAP se conectem ao banco de dados da rede ou diretório.
- ▶ Permite que consultem o banco de dados para obter informações sobre seus objetos.
- ▶ Ex: Um usuário na rede pode encontrar o número de telefone de outro usando o LDAP.

NetBIOS

- ▶ Usado para fazer chamadas de rede para sistemas remotos e funcionalidade de gerenciamento de sessão (como uma chamada telefônica).
- ▶ Protocolo de camada de sessão instalado com outros protocolos roteáveis.
- ▶ Dois modos de comunicação:
 - ▶ Modo de sessão (conexão full-duplex) ;
 - ▶ Modo datagrama (Não detecta erros, como broadcast).

Protocolos de Armazenamento de Rede

- ▶ **Fibre Channel**

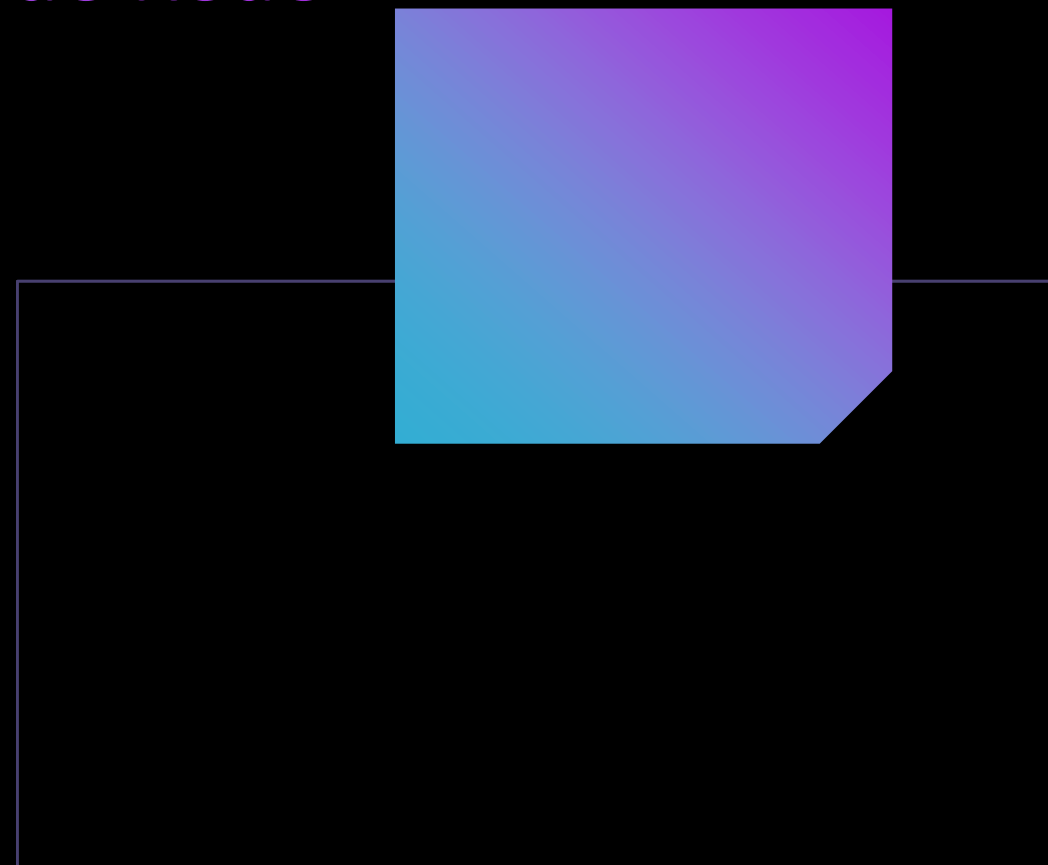
Tecnologia que transmite dados de até 128 Gbps e usa cabos ópticos especiais para conectar os dispositivos de armazenamento compartilhado aos servidores;

- ▶ **ISCSI**

Protocolo baseado em IP para comunicação com dispositivos de armazenamento; Não precisa de hardware especial como Fiber Channel.

- ▶ **FCoE**

Protocolo usado para transportar comandos Fibre Channel em uma rede Ethernet, mas não é roteável.



Entendendo o IPv6

IPv6

- ▶ Baseado em um esquema de endereço de 128 bits.
- ▶ Partes da Internet já utilizam o IPv6.
- ▶ Baseado em um esquema de endereços de 128 bits.
- ▶ Foco: suprir a escassez de endereços que existem com IPv4.

Endereços IPv6

Exemplo:

65b3:b834:45a3:0000:0000:762e:0270:5224

65b3:b834:45a3::762e:270:5224

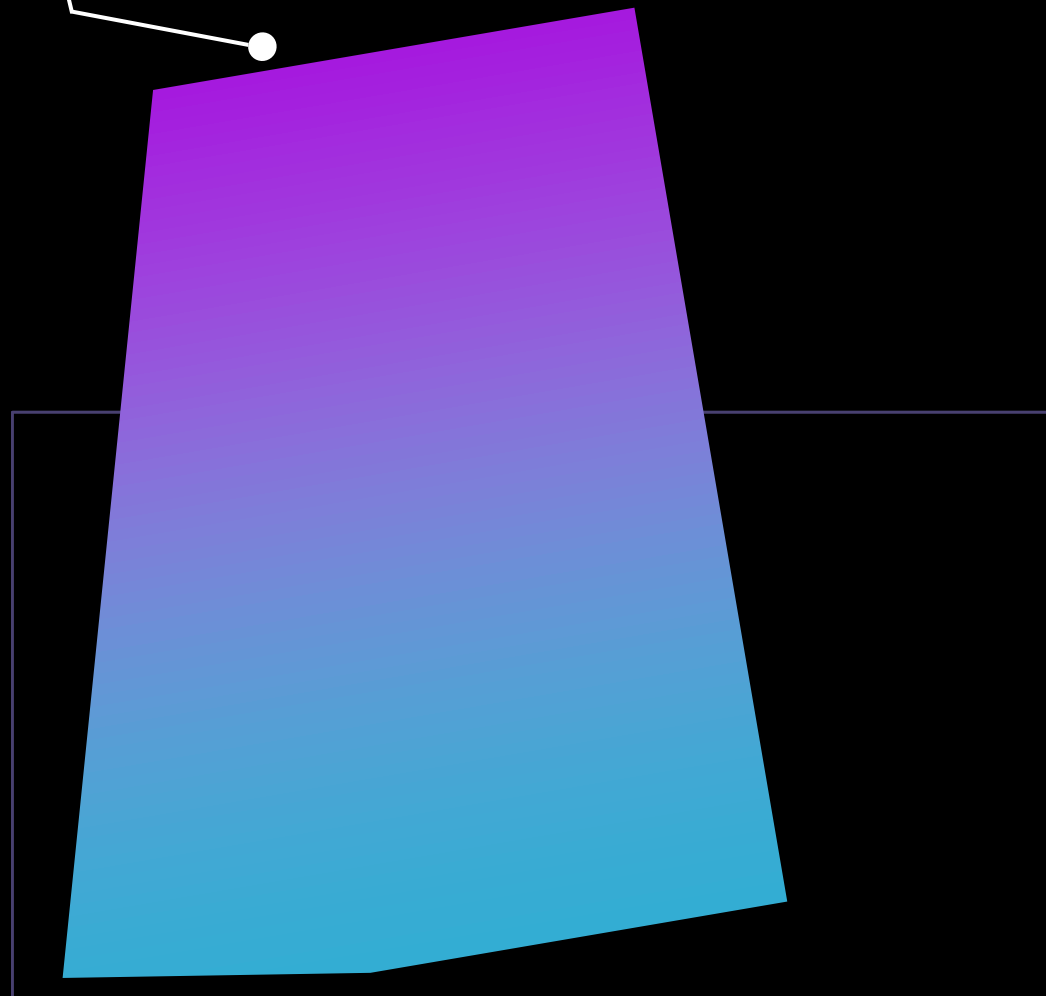
Não diferencia maiúsculas de minúsculas, e não há necessidade de zeros à esquerda.

Três tipos de endereços:

- ▶ Unicast;
 - ▶ Global unicast (público no IPv4);
 - ▶ Site-local unicast (privado no IPv4 "FEC0");
 - ▶ Link-local unicast (APIPA no IPv4 "FE80").
- ▶ Multicast (todas interfaces de um conjunto);
- ▶ Anycast (qualquer um do conjunto).

Protocolos IPv6

- ▶ **IPv6** - Responsável pelas funções de endereçamento e roteamento lógico (sem conexão, depende do TCP).
- ▶ **ICMPv6** - Responsável pelas informações de erro e status (Só usa código e não mais tipos).
- ▶ Descoberta de escuta de difusão seletiva (MLD), usado para Multicast, substituiu o IGMP;
- ▶ Neighbor Discovery (ND), substituindo o ARP.



Implicações do IPv6



Falta de conhecimento;



Complexidade do protocolo;



Suporte a dispositivos de segurança IPv6;

IPv4
IPv6

Vulnerabilidades de pilha dupla.

Segurança Física



- ▶ Todos os servidores devem ser armazenados em um lugar seguro;
- ▶ Controle e monitoramento do acesso aos componentes físicos.

Não Use Hubs

- ▶ A maioria dos ambientes está usando switches em vez de hubs.
- ▶ Certifique de substituir os hubs antigos por um switch.
- ▶ O tráfego precisa ser enviado para a porta na qual o sistema de destino reside.

Configurar Senhas

- ▶ Utilize a configuração de senhas para controlar quem está autorizado a administrar o dispositivo.
- ▶ Roteadores e switches Cisco têm várias senhas diferentes:



Senha da porta do console;



Senha da porta auxiliar;



Senhas Telnet.

```
HAL-R1 |>enable
HAL-R1 |#config term
HAL-R1 (config)|#line con 0
HAL-R1 (config-line)|#password Senh4P@$
HAL-R1 (config-line)|#login
```

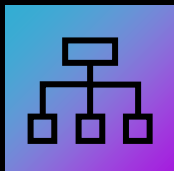
Copiar

Colar

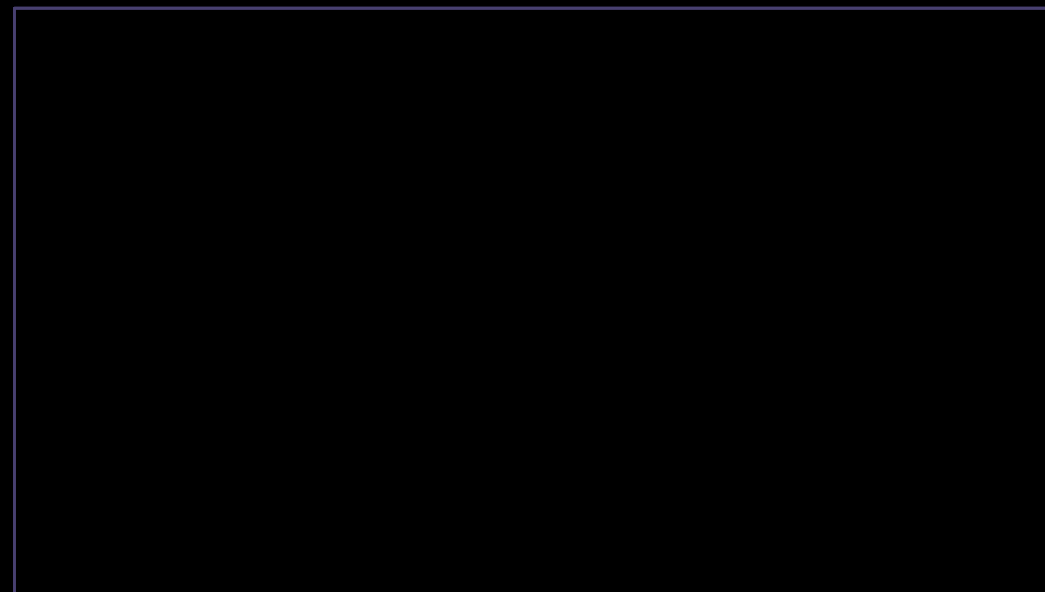
Use a Segurança da Porta

- ▶ As portas não usadas devem ser desabilitadas.
- ▶ Você deve configurar a segurança das portas.
- ▶ Método para especificar quais endereços MAC têm permissão para se conectar a uma determinada porta.
- ▶ A segurança da porta é uma contramedida contra a inundação de MAC, que faz com que duas coisas ocorram:
 - ▶ Switch enxerga todas as entradas como falsas no endereço MAC;
 - ▶ Entradas na tabela de endereços MAC são substituídas.

Usar VLANs



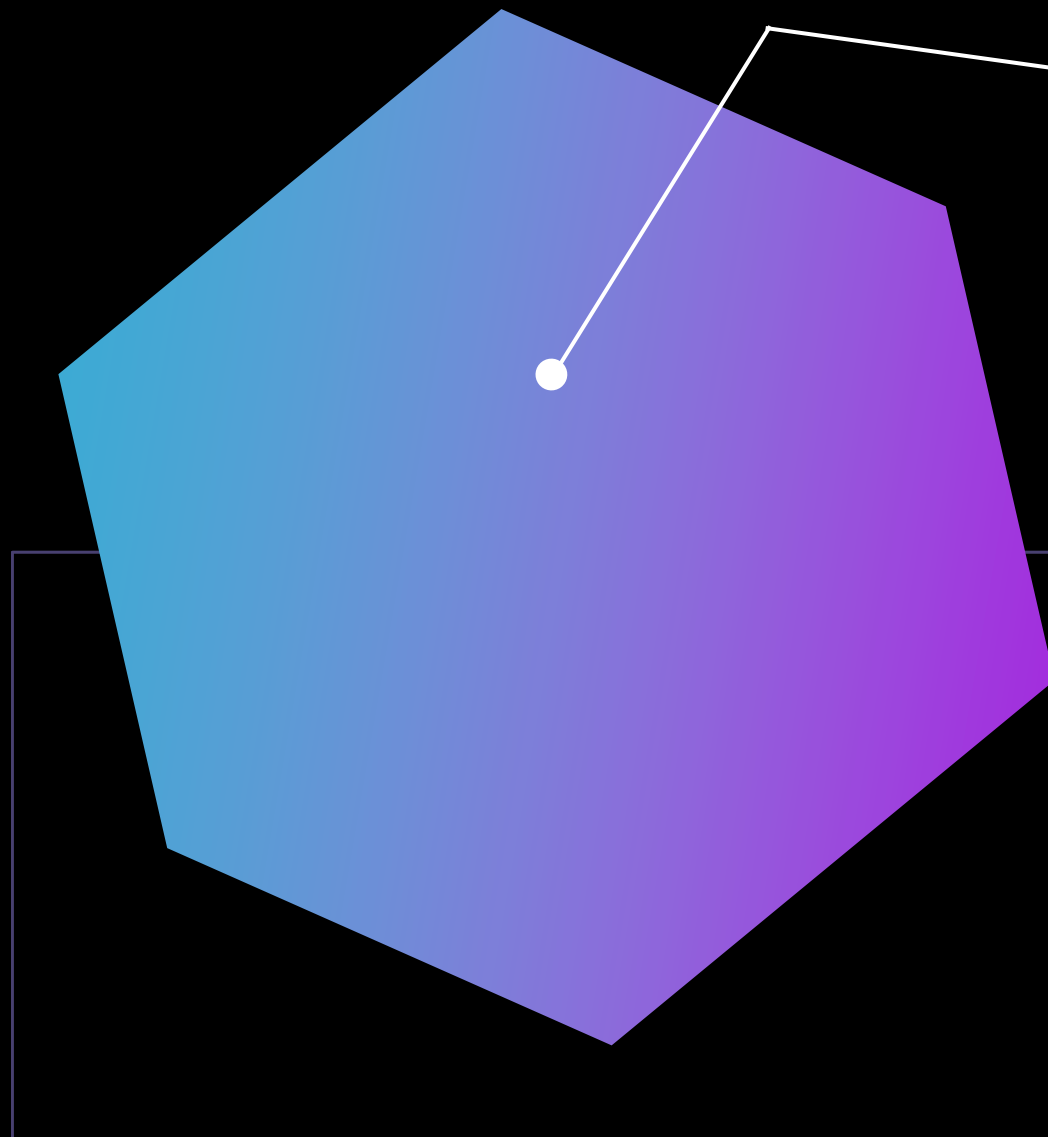
- ▶ As VLANs oferecem uma maneira de você criar diferentes limites de comunicação.
- ▶ Por padrão, um sistema que está em uma VLAN não pode se comunicar com sistemas em outra VLAN.



Uso de Cabo e Protocolo



- ▶ Você deve usar cabeamento de fibra ótica.
- ▶ Os dados transportados por cabos de cobre como um sinal elétrico são suscetíveis à interferência de outros componentes elétricos.
- ▶ Para protocolos, usá-los nos momentos em que mais se exige segurança.



OBRIGADO !

PROTOCOLOS DE CAMADA DE
APLICATIVO E PRÁTICAS RECOMENDADAS DE
SEGURANÇA DE REDE