

Na **Camada 4**, o cliente irritado geralmente diz: *"O ping está funcionando, então o problema é no servidor de vocês!"*. Ele confunde conectividade de rede (Camada 3) com disponibilidade de serviço (Camada 4).

Aqui, o problema será um **bloqueio de porta (Firewall)** impedindo o **Handshake TCP**, enquanto o ICMP (ping) passa livremente.

Cenário

- **O Problema:** O cliente não consegue acessar o acesso remoto (RDP - Porta **3389**) de um servidor crítico.
 - **O Cliente:** Um gestor de TI sob pressão, convencido de que o servidor "caiu", apesar de o ping responder.
-

A Simulação

Cliente: "Escuta aqui, eu não tenho o dia todo. O servidor de produção está fora do ar. Eu já testei daqui, ele está pingando, mas o Acesso Remoto não conecta de jeito nenhum. Já reiniciei minha máquina, já chamei o provedor e eles dizem que a rede está normal. Resolvam isso no servidor de vocês agora!"

Suporte N3 (Voz calma e segura): "Entendo a urgência, principalmente sendo um servidor de produção. Se o ping responde, a 'estrada' entre você e o servidor está aberta na Camada 3. Porém, o Acesso Remoto precisa de uma 'porta' específica aberta na Camada 4, a **3389**. Se o ping passa mas o RDP não, o problema está no aperto de mão (handshake) do TCP. Vamos verificar isso juntos?"

Cliente: "Porta? Handshake? Eu não quero aula de redes, eu quero acessar o servidor! Se o ping funciona, o IP está vivo. Se o IP está vivo, era para eu estar conectado. É óbvio que o serviço de vocês travou!"

Suporte N3: "Eu entendo seu ponto, mas veja só: o ping usa o protocolo ICMP, que não usa portas. Já o RDP usa **TCP**. É como se a estrada estivesse aberta, mas o portão da garagem estivesse trancado. Para não perdermos tempo reiniciando o servidor à toa, você pode rodar um comando rápido para mim? Digite `tnc [IP-do-Servidor] -port 3389` no seu PowerShell."

Cliente: "Vou fazer, mas já te aviso que vai dar erro... Pronto, deu aqui: `TcpTestSucceeded : False`. E agora? Vai admitir que o servidor quebrou?"

Suporte N3: "Isso confirma que o pacote **SYN** (o pedido de conexão) está sendo descartado antes de chegar ao serviço. Como o servidor está respondendo ao ping, eu acabei de checar o firewall de borda aqui. Alguém da sua equipe de segurança aplicou uma regra nova hoje de manhã?"

Cliente: "Segurança? Teve uma manutenção às 8h para fechar portas vulneráveis... Espera... Eles podem ter fechado a 3389 por engano?"

Suporte N3: "Exatamente o que aconteceu. O firewall está filtrando o tráfego TCP na porta 3389, mas permitindo o ICMP (ping). Por isso você vê o servidor 'vivo', mas não consegue 'conversar' com ele. Vou solicitar a liberação imediata dessa regra de transporte para o seu IP."

Cliente: (Silêncio por 3 segundos) "É... o pessoal da segurança fez uma alteração hoje cedo mesmo. Liberaram aqui agora e... conectou. Peço desculpas pelo tom, o estresse aqui está alto."

Suporte N3: "Sem problemas, eu entendo perfeitamente. Na Camada 4, esses bloqueios silenciosos são comuns. O importante é que o servidor está intacto e você já pode trabalhar. Algo mais em que eu possa ajudar?"

Análise Técnica da Camada 4 (L4) sob estresse:

1. **Diferença ICMP vs TCP:** O cliente achava que "Ping = Conexão Total". O Suporte N3 corrigiu mostrando que o **ICMP (L3)** pode funcionar enquanto o **TCP (L4)** é bloqueado.
2. **Handshake TCP (SYN, SYN-ACK, ACK):** O erro TcpTestSucceeded : False indicou que o pacote **SYN** nunca recebeu um **SYN-ACK**.
3. **Portas de Destino:** O diagnóstico focou na porta específica do serviço (**3389**) e não apenas no endereço IP.
4. **Firewall de Camada 4:** Diferente de um roteador simples, firewalls agem na L4 filtrando portas e protocolos específicos.

Ferramentas de Diagnóstico L4:

- **PowerShell:** Test-NetConnection -Port X
- **Telnet:** telnet [IP] [Porta] (clássico, mas em desuso)
- **Nmap:** Para scan de portas (usado com cautela em redes corporativas)
- **Netstat:** Para ver se o servidor está "ouvindo" (listening) na porta.

