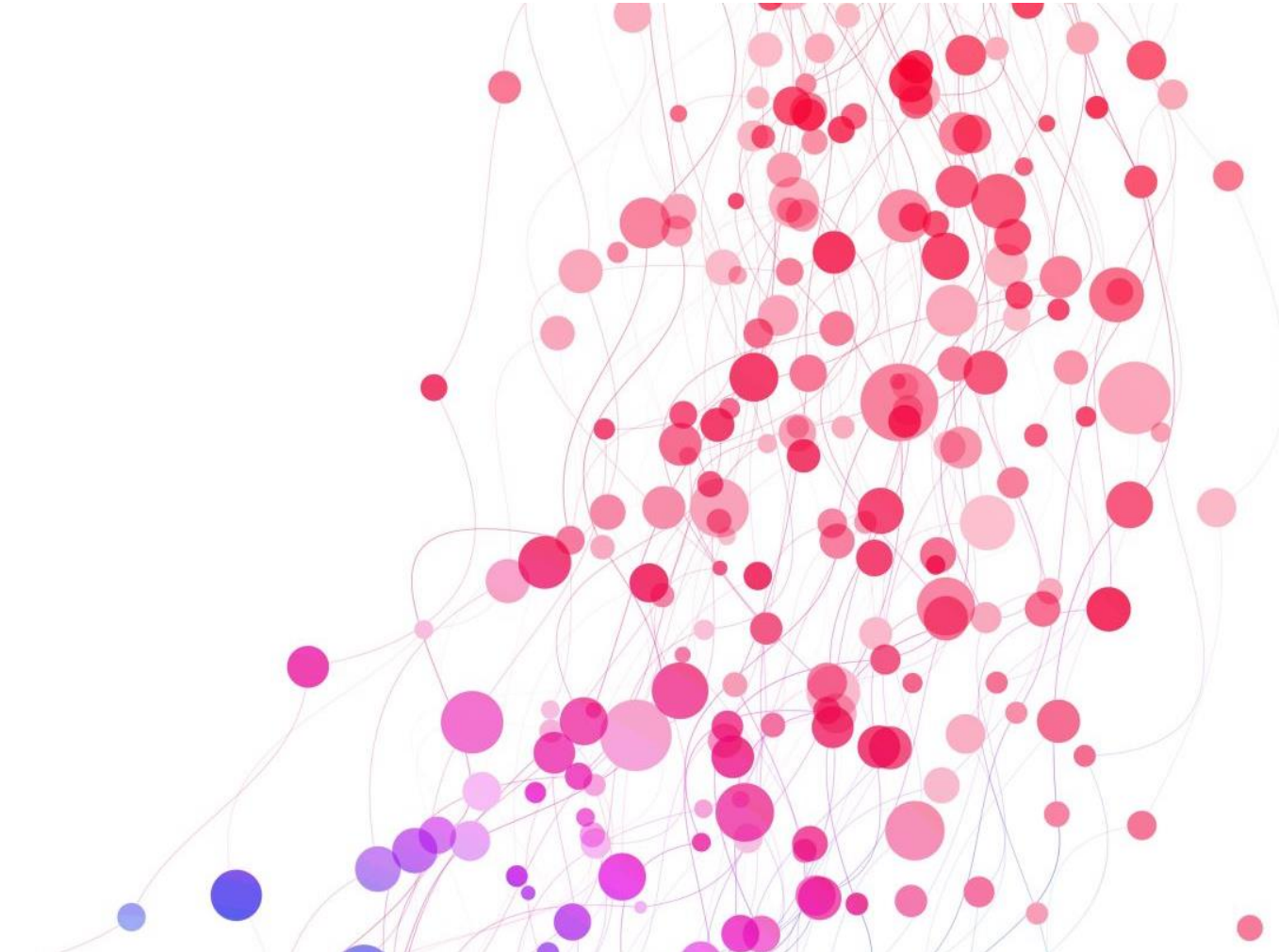
Administração Básica de Redes de Computadores
Continuação

PROF. RICARDO MESQUITA



Estratégias para o Firewall

- Existem dois tipos básicos de cenários de firewall:
  - proteger máquinas individuais (onde você define regras na cadeia INPUT de cada máquina)
  - proteger uma rede de máquinas (onde você define regras na cadeia FORWARD do roteador).
- Em ambos os casos:
  - você não pode ter segurança **séria** se usar uma política padrão de ACCEPT e inserir continuamente regras para descartar pacotes de fontes que começam a enviar coisas ruins.
  - Você deve *permitir apenas os pacotes em que confia e negar todo o resto*.

Estratégias para o Firewall

- Por exemplo, digamos que sua máquina tenha um servidor SSH na porta TCP 22, então:
  - *Não há razão* para qualquer host aleatório iniciar uma conexão com qualquer outra porta em sua máquina, e
  - Você *não deve dar chance* a esse host.
  - Para configurar isso, primeiro defina a política da cadeia INPUT como DROP:

```
# iptables -P INPUT DROP
```

Atenção: *Não execute* esse comando em uma máquina à qual você só tenha acesso remoto! O primeiro comando DROP *bloqueará instantaneamente* o seu acesso e você *não poderá recuperá-lo* até intervir (por exemplo, reiniciando a máquina).

Estratégias para o Firewall

- Para habilitar o tráfego ICMP (para ping e outros utilitários), use:

```
# iptables -A INPUT -p icmp -j ACCEPT
```

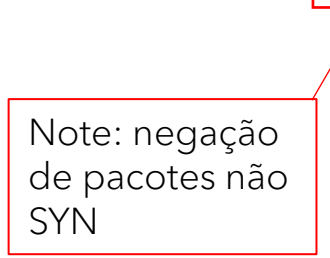
- Certifique-se de que você pode receber pacotes enviados para seu próprio endereço IP de rede e 127.0.0.1 (localhost).
- Supondo que o endereço IP do seu host seja my_addr, faça o seguinte:

```
# iptables -A INPUT -s 127.0.0.1 -j ACCEPT

# iptables -A INPUT -s my_addr -j ACCEPT
```

Estratégias para o Firewall

- Se você controla toda a sua sub-rede (e confia em tudo nela), você pode substituir my_addr pelo seu endereço de sub-rede e máscara de sub-rede (por exemplo, 10.23.2.0/24).
- Embora você ainda queira negar conexões TCP de entrada, você ainda precisa ter certeza de que seu host pode fazer conexões TCP com o mundo externo.
- Como todas as conexões TCP começam com um pacote SYN (solicitação de conexão), se você permitir a passagem de todos os pacotes TCP que não sejam pacotes SYN, você ainda estará bem:

```
# iptables -A INPUT -p tcp '!' --syn -j ACCEPT
```



Estratégias para o Firewall

- Em seguida, se estiver usando DNS remoto baseado em UDP, você deverá aceitar o tráfego do seu servidor de nomes para que sua máquina possa procurar nomes com DNS.
- Faça isso para todos os servidores DNS em /etc/resolv.conf.
- Use o seguinte comando (onde o endereço do servidor de nomes é ns_addr):

```
# iptables -A INPUT -p udp --source-port 53 -s ns_addr -j ACCEPT
```

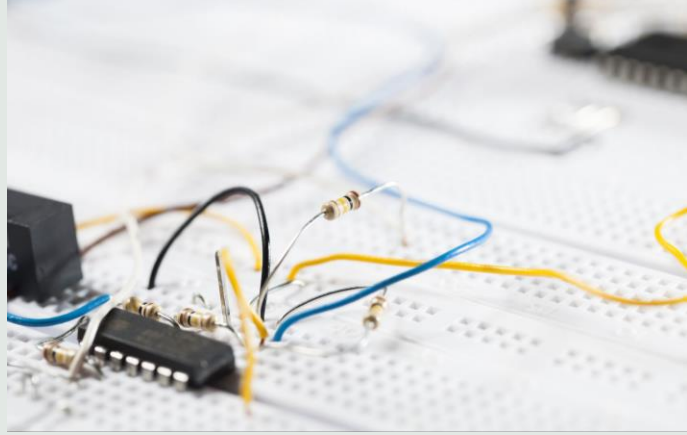
- Finalmente, permita conexões SSH de qualquer lugar:

```
# iptables -A INPUT -p tcp --destination-port 22 -j ACCEPT
```

Estratégias para o Firewall

- As configurações do iptables funcionam para muitas situações, incluindo qualquer conexão direta (especialmente banda larga) onde um intruso tem muito mais probabilidade de fazer uma varredura de porta em sua máquina.
- Você também pode adaptar essas configurações para um roteador de firewall usando a cadeia FORWARD em vez de INPUT e usando sub-redes de origem e destino quando apropriado.
- Para configurações mais avançadas, você pode achar útil uma ferramenta de configuração (p.ex., Shorewall - https://shorewall.org/).

Ethernet, IP, ARP e NDP



- Lembre-se:
  - Um host deve colocar um pacote IP dentro de um quadro Ethernet para poder transmitir o pacote através da camada física para outro host.
  - Os frames não incluem informações de endereço IP; eles usam endereços MAC (hardware).
- Então, ao construir o quadro Ethernet para um pacote IP, como o host sabe qual endereço MAC corresponde ao endereço IP de destino?
- O software de rede inclui um sistema automático de procura de endereços MAC.
  - No IPv4, isso é chamado de Protocolo de Resolução de Endereços (ARP).
- O host que usa Ethernet e IP mantém uma pequena tabela chamada cache ARP que mapeia endereços IP para endereços MAC.

Ethernet, IP, ARP e NDP

- No Linux, o cache ARP está no kernel.
- Para visualizar o cache ARP da sua máquina, use o comando **ip neigh**. (O comando antigo para trabalhar com o cache ARP é **arp**.)

```
$ ip -4 neigh
10.1.2.57 dev enp0s31f6 lladdr 1c:f2:9a:1e:88:fb REACHABLE
10.1.2.141 dev enp0s31f6 lladdr 00:11:32:0d:ca:82 STALE
10.1.2.1 dev enp0s31f6 lladdr 24:05:88:00:ca:a5 REACHABLE
```

- Note:
  - O -4 restringe a saída ao IPv4.
  - REACHABLE: ocorreu comunicação recentemente e
  - STALE: já há algum tempo sem comunicação e a entrada deve ser atualizada.

Ethernet, IP, ARP e NDP

- arp x ip neigh

$ arp

Address	HWtype	HWaddress	Flags	Mask	Iface
mh9-imac.fritz.box	ether	00:25:4b:9b:64:49	C		wlp1s0
fritz.box	ether	3c:a6:2f:8e:66:b3	C		

$ ip neigh

192.168.178.34 dev wlp1s0 lladdr 00:25:4b:9b:64:49 STALE

192.168.178.1 dev wlp1s0 lladdr 3c:a6:2f:8e:66:b3 REACHABLE

Ethernet, IP, ARP e NDP

- Quando uma máquina é inicializada, seu cache ARP fica vazio.
- Se um endereço IP de destino não estiver em um cache ARP, ocorrerão as seguintes etapas:
  1. O host de origem cria um quadro Ethernet especial contendo um pacote de solicitação ARP para o endereço MAC que corresponde ao endereço IP de destino.
  2. O host de origem transmite esse quadro para toda a rede física da sub-rede de destino.
  3. Se um dos outros hosts na sub-rede souber o endereço MAC correto, ele criará um pacote de resposta e um quadro contendo o endereço e os enviará de volta à origem.
  4. O host de origem adiciona o par de endereços IP-MAC ao cache ARP e pode prosseguir.

Ethernet, IP, ARP e NDP

Atenção:

- Lembre-se de que o ARP se aplica apenas a máquinas em sub-redes locais!
- Para alcançar destinos fora da sua sub-rede, seu host envia o pacote para o roteador, e depois disso o problema é de outra pessoa.
- É claro que seu host ainda precisa saber o endereço MAC do roteador e pode usar ARP para encontrá-lo.

Ethernet, IP, ARP e NDP

- O único problema real que você pode ter com o ARP é que o cache do seu sistema pode ficar desatualizado se você mover um endereço IP de uma placa de interface de rede para outra porque as placas têm endereços MAC diferentes.
- Os sistemas Unix invalidam as entradas de cache ARP se não houver atividade após um tempo, portanto não deverá haver nenhum problema além de um pequeno atraso para dados invalidados, mas você pode excluir uma entrada de cache ARP imediatamente com o seguinte comando:

```
# ip neigh del host dev interface
```

Ethernet, IP, ARP e NDP

- No IPv6, há um novo mecanismo chamado *Neighbor Discovery Protocol* (NDP) usado na rede link-local.
- O comando ip unifica ARP de IPv4 e NDP de IPv6.
- O NDP inclui estes dois tipos de mensagens:
  - Solicitação de vizinho: usada para obter informações sobre um host de link local, incluindo seu endereço de hardware.
  - Anúncio de vizinho: usado para responder a uma mensagem de solicitação de vizinho.

Wireless Ethernet

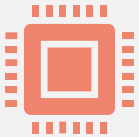
- O kernel do Linux pode se comunicar com uma interface de rede sem fio da mesma forma que faria com uma interface de rede com fio.
- Tudo na camada de rede e acima é igual; as principais diferenças são componentes adicionais na camada física, como frequências, IDs de rede e recursos de segurança.
- Ao contrário do hardware de rede com fio, que é muito bom em se ajustar automaticamente às nuances da configuração física, a configuração da rede sem fio é muito mais aberta.
- Para que uma interface sem fio funcione corretamente, o Linux precisa de ferramentas de configuração adicionais.

Wireless Ethernet

- Detalhes de transmissão: são características físicas, tais como a frequência.
- Identificação da rede: como mais de uma rede sem fio pode compartilhar o mesmo meio básico, você precisa ser capaz de distingui-las.
  - O *Service Set Identifier* (SSID) é o identificador da rede sem fio.
- Gerenciamento: embora seja possível configurar redes sem fio para que os hosts se comuniquem diretamente entre si, a maioria das redes sem fio é gerenciada por um ou mais pontos de acesso pelos quais todo o tráfego passa.
- Os pontos de acesso: geralmente conectam uma rede sem fio a uma rede com fio, fazendo com que ambas pareçam uma única rede.
- Autenticação: para restringir o acesso a uma rede sem fio, você pode configurar pontos de acesso para exigir uma senha ou outra chave de autenticação.
- Criptografia: além de restringir o acesso inicial a uma rede sem fio, normalmente você deseja criptografar todo o tráfego que passa pelas ondas de rádio.

Wireless Ethernet

A configuração e os utilitários do Linux que lidam com esses componentes estão espalhados por diversas áreas.



Alguns estão no kernel; o Linux apresenta um conjunto de extensões sem fio que padronizam o acesso do espaço do usuário ao hardware.

No que diz respeito ao espaço do usuário, a configuração sem fio pode ficar complicada, então a maioria das pessoas prefere usar interfaces GUI, como o miniaplicativo de desktop do NetworkManager (https://networkmanager.dev), para fazer as coisas funcionarem.

iw

- Para visualizar e alterar o dispositivo de espaço do kernel e a configuração de rede você pode chamar o utilitário iw.
- Para usar o iw, normalmente você precisa saber o nome da interface de rede do dispositivo, como wlp1s0 (nome previsível do dispositivo) ou wlan0 (nome tradicional).
- Aqui está um exemplo que faz uma varredura nas redes sem fio disponíveis.

```
# iw dev wlp1s0 scan
```

Atenção:
- A interface de rede deve estar ativa para que este comando funcione (se não estiver, execute **ip link set wlp1s0 up**)
- Como ainda está na camada física, você não precisa configurar nenhum parâmetro da camada de rede, como um IP endereço.

iw

- Se a interface de rede tiver ingressado em uma rede sem fio, você poderá visualizar os detalhes da rede com:

```
# iw dev wlp1s0 link
```

- O endereço MAC na saída deste comando é do ponto de acesso com o qual você está conversando no momento.

Atenção:
- O comando iw distingue entre nomes de dispositivos físicos (como phy0) e nomes de interfaces de rede (como wlp1s0) e permite alterar várias configurações para cada um.
- Pode-se criar mais de uma interface de rede para um único dispositivo físico.
- No entanto, em quase todos os casos básicos, você usará apenas o nome da interface de rede.

iw

- Use iw para conectar uma interface de rede a uma rede sem fio não segura da seguinte forma:

```
# iw wlp1s0 connect network_name
```

- Para o sistema Wired Equivalent Privacy (WEP) bastante inseguro, você pode usar o parâmetro keys com o comando iw connect.
- No entanto, você não deve usar WEP porque não é seguro e você não encontrará muitas redes que o suportem.

iw

```
$ iw dev wlp1s0 info
Interface wlp1s0
        ifindex 2
        wdev 0x1
        addr 38:de:ad:37:32:0f
        ssid FRITZ!Box 7530 QJ
        type managed
        wiphy 0
        channel 5 (2432 MHz), width: 20 MHz, center1: 2432 MHz
        txpower 20.00 dBm
```

Interface wireless

O roteador ao qual a interface está conectada

A frequência de banda WiFi que a interface está usando.

iw

- Pode-se também coletar informações relacionadas com o tráfego.

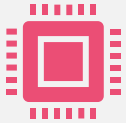
```
$ iw dev wlp1s0 link
Connected to 74:42:7f:67:ca:b5 (on wlp1s0)
        SSID: FRITZ!Box 7530 QJ
        freq: 2432
        RX: 28003606 bytes (45821 packets)
        TX: 4993401 bytes (15605 packets)
        signal: -67 dBm
        tx bitrate: 65.0 MBit/s MCS 6 short GI

        bss flags:      short-preamble short-slot-time
        dtim period:    1
        beacon int:     100
```

Mostrar informações de conexão sobre a interface sem fio wlp1s0.

Estas linhas mostram estatísticas de envio (TX significa "transmitir") e recebimento (RX), ou seja, bytes e pacotes enviados e recebidos por meio desta interface.

Segurança em meio Wireless

Dica importante:
Use softwares de apoio para configuração adequada (p.ex. NetworkManager).



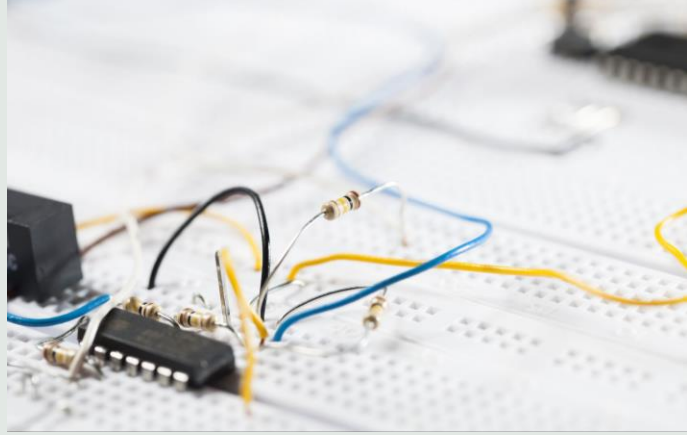
Para a maioria das configurações de segurança sem fio, o Linux depende do daemon wpa_supplicant para gerenciar a autenticação e a criptografia de uma interface de rede sem fio.

Este daemon pode lidar com os esquemas de autenticação WPA2 e WPA3 (WiFi Protected Access. ATENÇÃO: não use os antigos e inseguros WPA), bem como quase qualquer tipo de técnica de criptografia usada em redes sem fio.

Quando o daemon é iniciado pela primeira vez, ele lê um arquivo de configuração (por padrão, /etc/wpa_supplicant.conf) e tenta se identificar em um ponto de acesso e estabelecer comunicação com base em um determinado nome de rede.

Se sistema está bem documentado; em particular, a página de manual wpa_supplicant é muito detalhada.

Network Interface Controller



- Placa de interface de rede.
- A NIC fornece conectividade física a uma rede por meio de um padrão com fio (por exemplo, o padrão IEEE 802.3-2018 para Ethernet) ou de um dos muitos padrões sem fio da família IEEE 802.11.
- Transforma a representação digital dos bytes que você deseja enviar em sinais elétricos ou eletromagnéticos.
- Também transforma quaisquer sinais físicos recebidos em bits e bytes com os quais o software pode lidar.

Network Interface Controller

- Vamos ver um exemplo com **ifconfig** (obsoleto):

```
$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536 1
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 7218  bytes 677714 (677.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7218  bytes 677714 (677.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500 2
        inet 192.168.178.40  netmask 255.255.255.0  broadcast 192.168.178.255
        inet6 fe80::be87:e600:7de7:e08f  prefixlen 64  scopeid 0x20<link>
        ether 38:de:ad:37:32:0f  txqueuelen 1000  (Ethernet)
        RX packets 2398756  bytes 3003287387 (3.0 GB)
        RX errors 0  dropped 7  overruns 0  frame 0
        TX packets 504087  bytes 85467550 (85.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

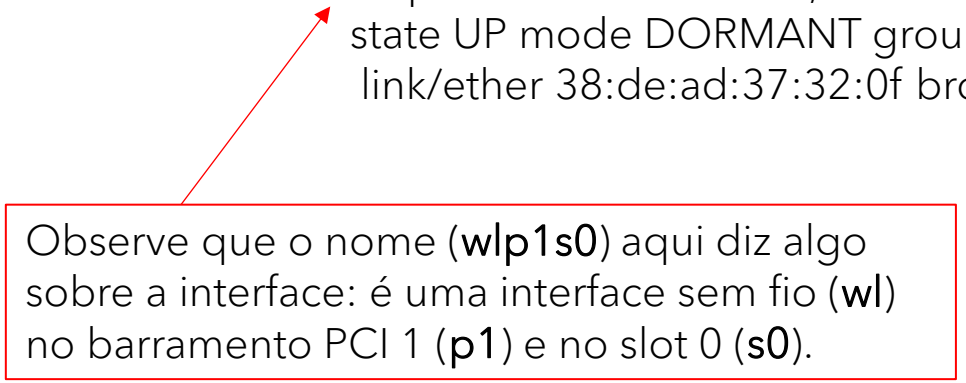
- Interface de loopback com o endereço IP 127.0.0.1
- MTU de 65.536 bytes (tamanhos maiores significam maiores rendimentos)

- Interface NIC com seu endereço MAC (ether 38:de:ad:37:32:0f).
- Os sinalizadores (<UP,BROADCAST,RUNNING,MULTICAST>) sugerem estar operacional.

Network Interface Controller

- Para uma abordagem mais moderna de fazer a mesma coisa (consultar interfaces e verificar seu status), use o comando ip.

```
$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue 1
   state UNKNOWN mode DEFAULT group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: wlp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue 2
   state UP mode DORMANT group default qlen 1000
    link/ether 38:de:ad:37:32:0f brd ff:ff:ff:ff:ff:ff
```



Dúvidas?