Fundamentos de Segurança Informática (FSI)

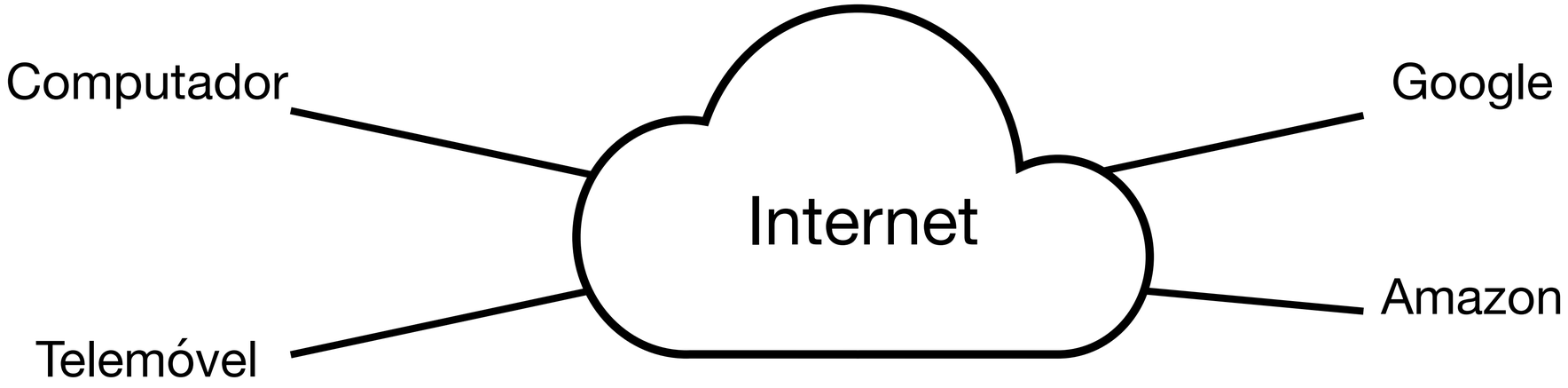
2021/2022 - LEIC

Manuel Barbosa
mbb@fc.up.pt

Aula 21
Segurança de Redes 1

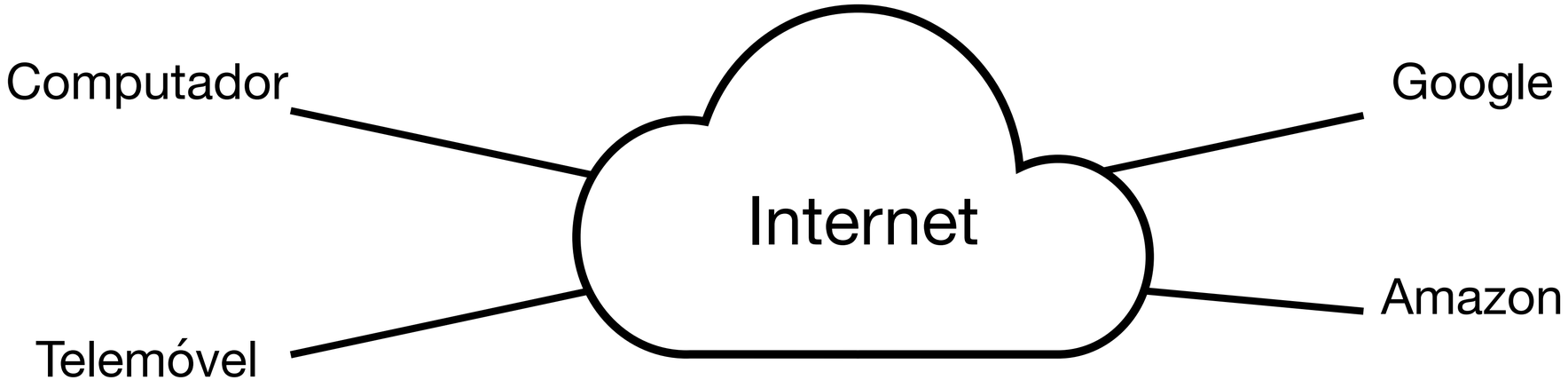
Recap

A Rede



- Ideia original:
  - rede simples/básica onde cada máquina/host tem um endereço IP
  - complexidade nos pontos terminais (endpoints)
  - funciona como um correio: entrega pacotes <> ligações físicas comutadas

A Rede



- Para comunicar precisamos de regras = protocolos:
  - sintaxe: especificação da estrutura das mensagens, ordem, formato
  - semântica: qual o significado de uma mensagem, ação a desencadear
  - normas/especificações: todos partilham as mesmas regras

Modelo OSI: Camadas = Encapsulamento

OSI Model				
Layer		Data unit	Function[3]	Examples
Host layers	7. Application	Data	High-level APIs, including resource sharing, remote file access, directory services and virtual terminals	HTTP, FTP, SMTP
	6. Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption	
	5. Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes	RPC, PAP
	4. Transport	Segments	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing	TCP, UDP
Media layers	3. Network	Packet/Datagram	Structuring and managing a multi-node network, including addressing, routing and traffic control	IPv4, IPv6, IPsec, AppleTalk, ICMP
	2. Data link	Bit/Frame	Reliable transmission of data frames between two nodes connected by a physical layer	PPP, IEEE 802.2, L2TP
	1. Physical	Bit	Transmission and reception of raw bit streams over a physical medium	DSL, USB

Arquitetura em Ampulheta

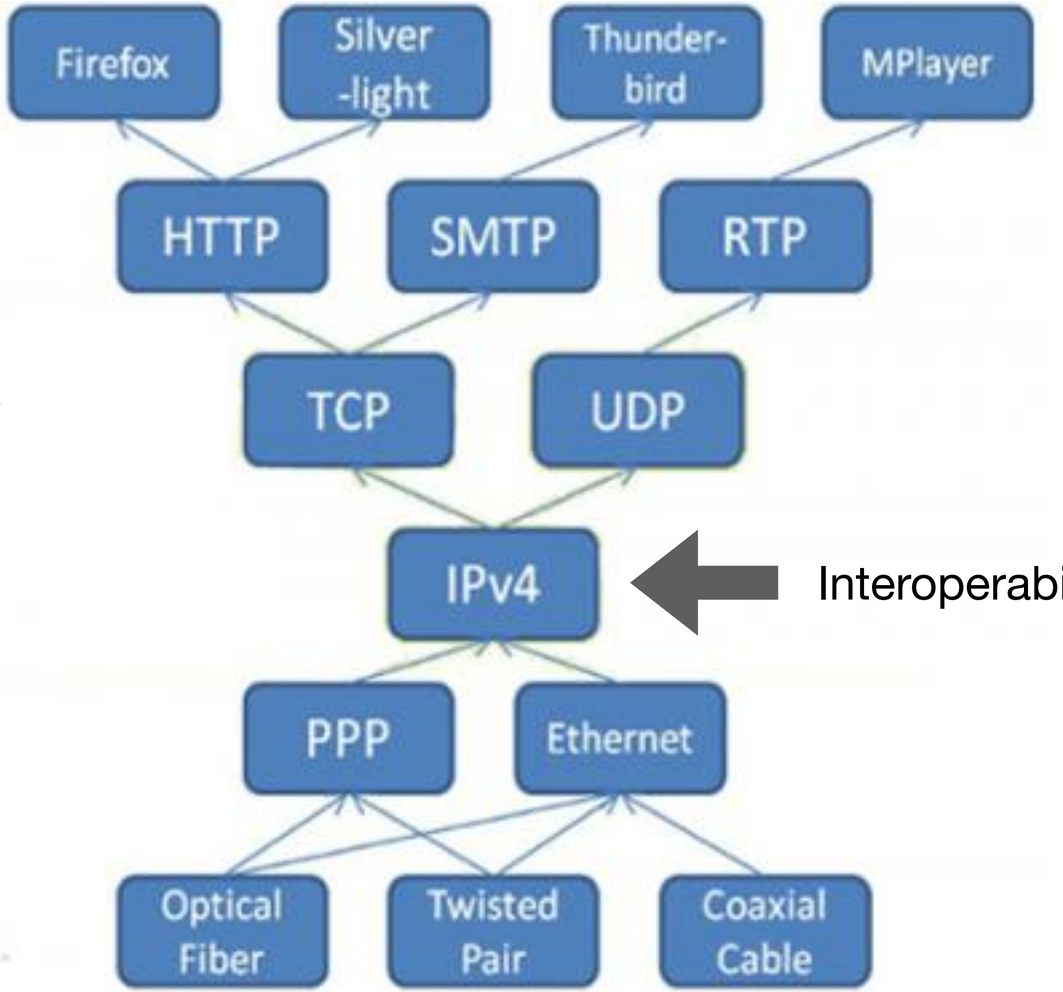
como é que as aplicações estruturam a informação?

como acedo ao serviço correto? como tenho um stream fiável?

como é que um pacote chega de uma máquina a outra?

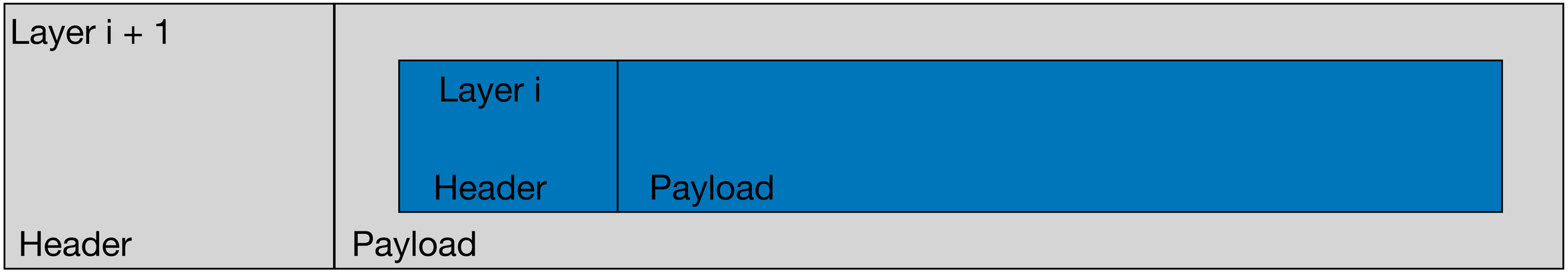
como é que eu salto de uma rede local para outra?

como é que a informação se transmite fisicamente?

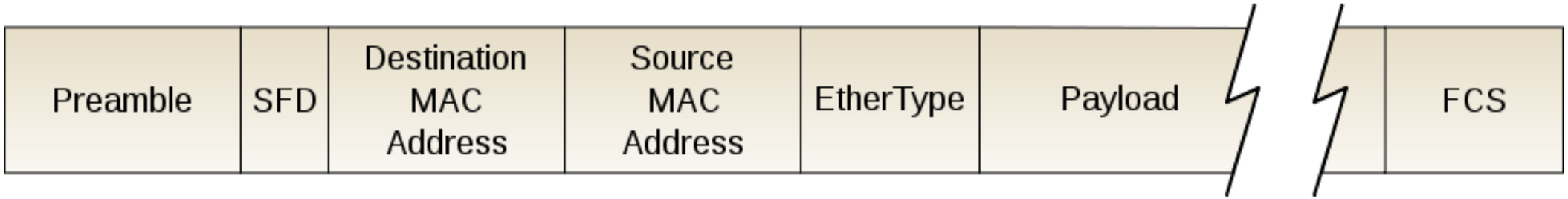


Dispositivos

- Camada física: hubs, repetidores, antenas, cabos
- Camada lógica: switches, bridges
- Camada de rede: routers
- Camada de transporte e superior: gateways



Ethernet: Link Layer mais Comum



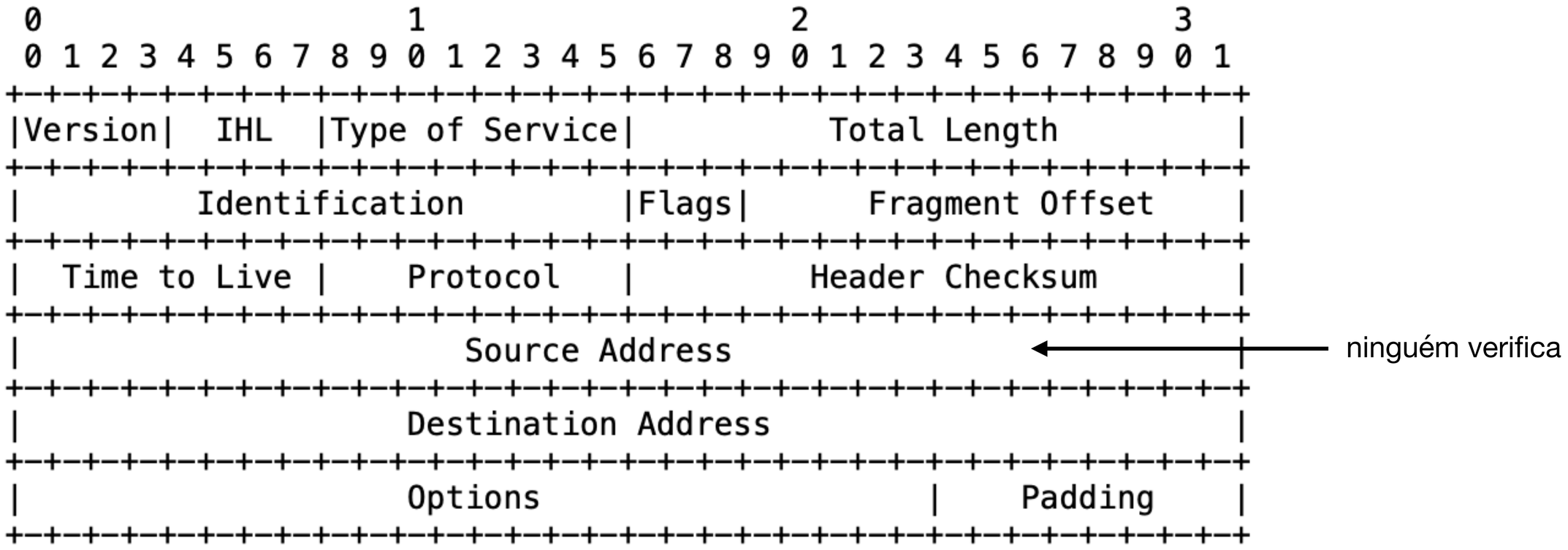
- Mensagens = frames => EtherType permite identificar protocolo de rede (IP, ARP, etc.)
- Cada nó tem um endereço MAC (Media Access Control) = 6 bytes
- Localmente broadcast => escalabilidade usando switch
- WiFi funciona de maneira semelhante, mas os nós são móveis

From Wikipedia

Protocolo IP

- Comunicação sem “ligação”
  - Best-effort: não há garantias de entrega
  - Não há tentativas de recuperação
  - Pacotes podem perder-se, ser permutados, repetidos, etc.
- Pacotes podem mesmo ser fragmentados
- Estrutura de endereços hierárquica (IPv4 = 32 bits, IPv6 = 128-bits)
  - Endereço atribuído de forma estática ou dinamicamente via DHCP

Um cabeçalho IP



https://datatracker.ietf.org/doc/html/rfc791#page-11

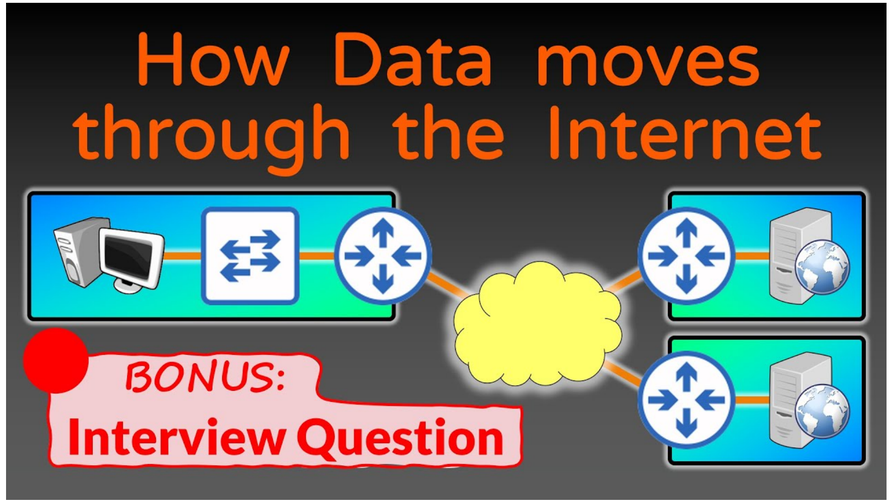
Perguntas

- Localmente: como sabemos os endereços MAC uns dos outros?
- Internet: como é que os routers sabem para onde enviar os pacotes?

Comunicação na Internet

- Dentro de uma sub-rede local:
  - Comunicação com base em MAC address
  - Switch optimiza distribuição de pacotes na rede local (recorda endereços MAC)
  - Tabela de endereços MAC: construída com pedidos/anúncios Address Resolution (ARP):
    - pedido = meu MAC + quem tem este IP?
    - resposta = meu MAC + teu MAC + meu IP

Ver este vídeo



https://www.youtube.com/watch?v=YJGGYKAV4pA

Routing de pacotes

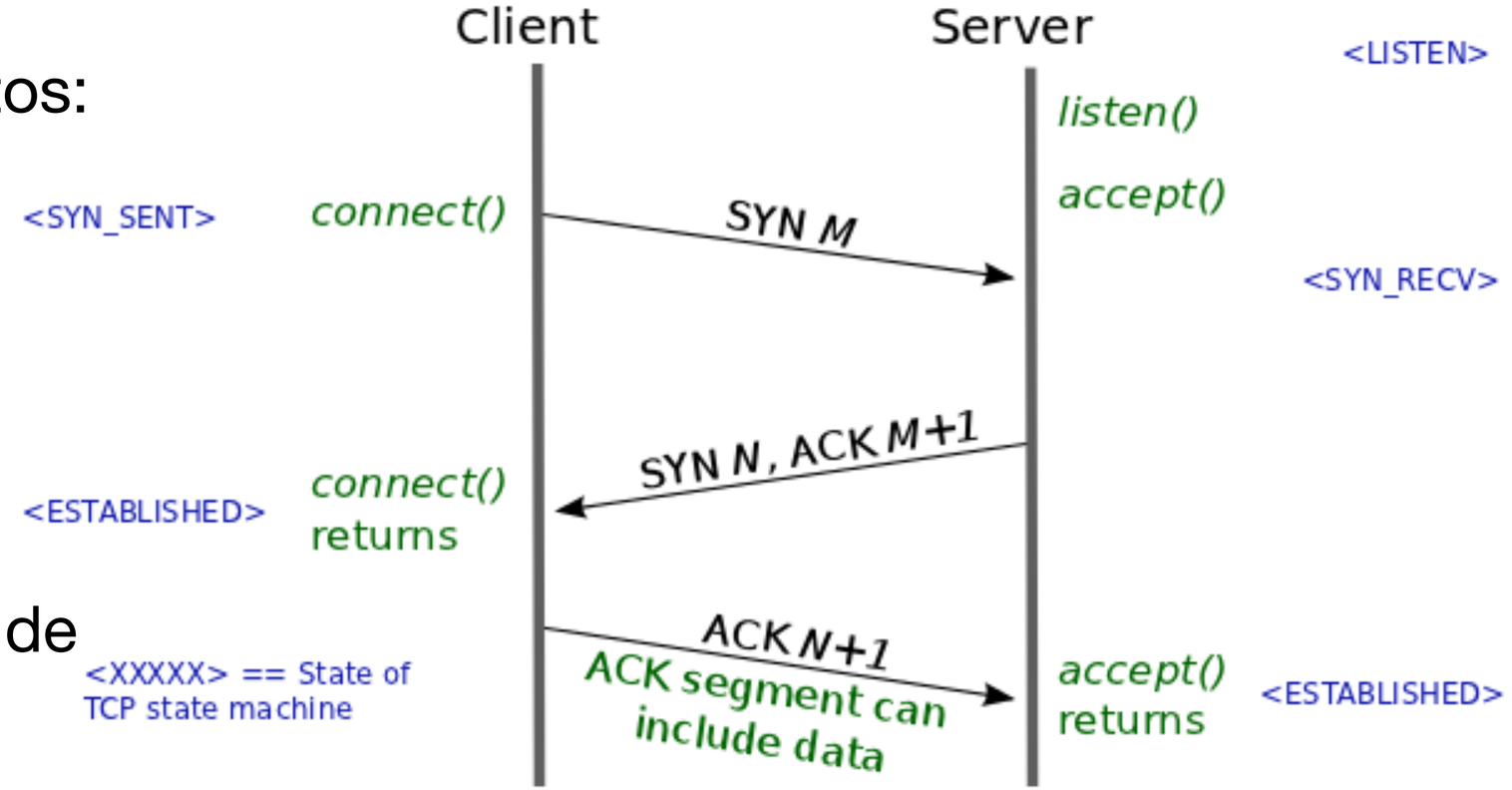
- Os routers encaminham pacotes com base em tabelas: localmente gerida por *sysadmins*
- Globalmente: routing baseado no Border Gateway Protocol
  - Internet organizada em Autonomous Systems (AS)
  - Estrutura quasi-hierárquica com um pequeno número de AS de topo
  - Configuração automática de tabelas de routing (muito complexo)
    - cada router mantém tabela de routing global
    - routers anunciam a outros routers o que podem encaminhar
    - os encaminhamentos são propagados pela rede

Protocolo TCP

- Comunicação fiável entre aplicações em máquinas diferentes:
  - ligações de longa duração, streams de bytes => uma em cada direção
  - conexão, desconexão explícitos
  - gestão de tráfego/congestão
- Aplicações identificadas por um número de porta (16 bits)
- Algumas portas são reservadas: 80, 443, 25, 22, etc.

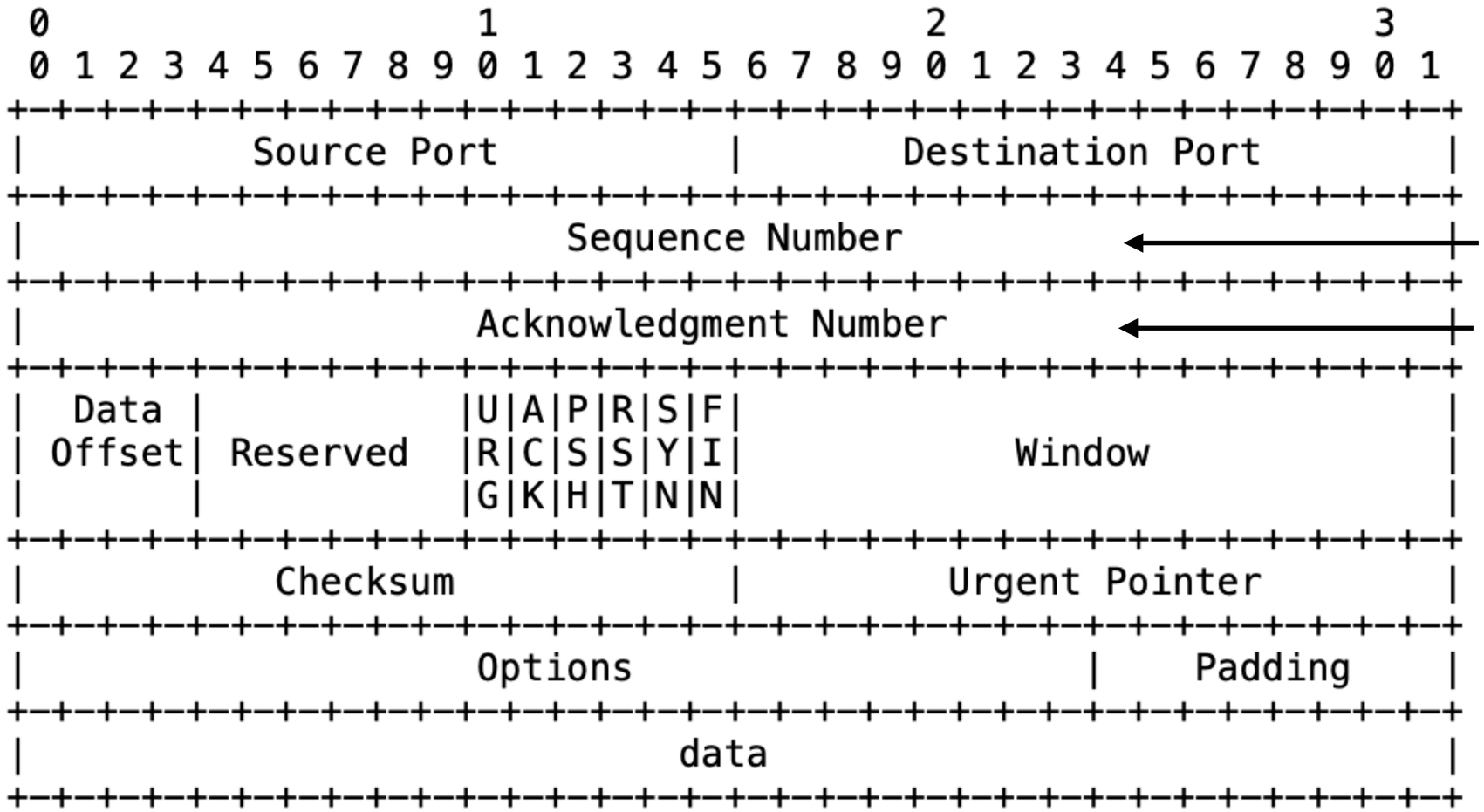
Handshake e Comunicações TCP

- Ligações geridas com base em números de sequência (32-bits)
- Dados enviados em segmentos: 1 segmento = 1 pacote IP
- Receptor confirma (ACK) receção dos dados
- Emissor pode retransmitir e adaptar cadência em função de timeouts



https://lwn.net/Articles/508865/

Um cabeçalho TCP



codifica posição no byte stream

confirma receção de prefixo no stream

handshake fixa seqn inicial
trocas seguintes aumentam número de sequência com base em número de bytes transmitidos/ recebidos

https://datatracker.ietf.org/doc/html/rfc793#page-15

Mais TCP

- Flag FIN termina a ligação (implica ACK)
- Flag RST permite a cliente terminar ligação sem ACK (detetou um erro)
- Recordar: UDP = Wrapper do IP sem ligações/gestão do TCP

https://lwn.net/Articles/508865/

Domain Name Service (DNS)

- Permite mapear nomes legíveis (hierárquicos) em endereços IP (usa UDP)
- ~13 servidores DNS de raiz com visão completa
  - nós hierarquicamente inferiores têm visão parcial
  - resolução feita subindo na hierarquia e perguntando à autoridade correspondente (podemos ter de fazer vários pedidos)
  - caching de resultados para eficiência

```
$ dig fc.up.pt

; <<>> DiG 9.10.6 <<>> fc.up.pt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR,
id: 38203
;; flags: qr rd ra; QUERY: 1, ANSWER: 1,
AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4010
;; QUESTION SECTION:
;fc.up.pt.          IN  A

;; ANSWER SECTION:
fc.up.pt.       3600    IN  A   193.137.24.4

;; Query time: 25 msec
;; SERVER:
2001:8a0:ffb0:f300::1#53(2001:8a0:ffb0:f300::1)
;; WHEN: Mon Dec 27 11:48:13 WET 2021
;; MSG SIZE  rcvd: 53
```

Segurança

Modelo CIA

- Confidencialidade, Integridade, Disponibilidade (recordar o que são)
- Ataques potenciais em todos os níveis da rede e com diversos níveis de intervenção:
  - Físico, ligação direta ao meio de comunicação
  - Dispositivos manipulados/configurados para realizar ataques
  - Infraestruturas elaboradas de vigilância e controlo de comunicações

Os adversários

- Veremos que, ao nível das comunicações, existe pouca ou nenhuma proteção:
  - atacantes que podem observar comunicações (eavesdropper)
  - atacantes que podem inserir pacotes (off path)
  - atacantes que podem observar e inserir pacotes (on path)
  - atacantes que podem controlar todas as comunicações (man in the middle)
- Para ter proteção na Internet é necessário utilizar criptografia:
  - TLS, IPSec, etc.

Camada física/lógica

Wiretapping

- Wiretapping é o processo de escutar um canal de comunicações onde entidades terceiras estão a trocar informação
- O atacante liga um equipamento seu ao meio de comunicação para poder recolher informação
- No wiretapping activo (ao contrário do passivo) o atacante pode mesmo injectar, modificar informação, ou fazer DoS (e.g., jamming)
- O wiretapping está institucionalizado em muitos países, como forma de monitorização dos serviços de segurança

Eavesdropping/Packet sniffing

- É uma forma de wiretapping em redes de comunicação, onde se recolhem e armazenam os pacotes trocados entre utilizadores legítimos de uma sub-rede
- Permite a um atacante observar todas as comunicações não cifradas
  - extrair passwords e outra informação sensível
- Para isso basta ter acesso ao meio de comunicação e uma interface de rede capaz de funcionar em modo promíscuo:
  - em redes wireless desprotegidas é trivial
  - em redes wireless protegidas, credenciais de acesso dão acesso e por vezes permitem wiretapping total (detalhes em aula futura)
  - em redes físicas, basta ter um ponto de acesso a uma tomada de rede

Ferramentas

- Existe hardware especializado para sniffing, com capacidade para lidar com ligações de alto débito
- Muitas destas ferramentas são criadas para auxiliar os técnicos que montam as infra-estruturas
- Existem também ferramentas em software que funcionam tão melhor quanto melhor for o equipamento disponível
- Ver por exemplo o (e.g., tcpdump, wireshark)

NEWS

Russian agents inspect undersea cables in Ireland amid fears they could tap into or tamper with links to US

https://www.irishpost.com/news/russian-agents-inspect-undersea-cables-ireland-amid-fears-tap-tamper-links-us-179836

As revelações Snowden

Optic Nerve (GCHQ)

From Wikipedia, the free encyclopedia

Optic Nerve is a mass surveillance programme run by the British signals intelligence agency Government Communications Headquarters (GCHQ), with help from the US National Security Agency, that surreptitiously collects private webcam still images from users while they are using a Yahoo! webcam application. As an example of the scale, in one 6-month period, the programme is reported to have collected images from 1.8 million Yahoo! user accounts globally. The programme was first reported on in the media in February 2014, from documents leaked by the former National Security Agency contractor Edward Snowden, but dates back to a prototype started in 2008, and was still active in at least 2012.[1][2]

MAC flooding: melhor sniffing

- Hoje em dia quase todas as redes são switched
- Um switch mantém uma tabela dos endereços MAC que estão em cada segmento
- Utiliza esta informação para optimizar a transmissão de pacotes
- Injectando mensagens com MACs novos na rede, estas tabelas são esvaziadas dos endereços reais
- O switch começa então a retransmitir todos os pacotes permitindo obter um sniffing mais eficaz
- O switch passa a funcionar como um hub (equipamento menos elaborado)
- O ataque também afecta switches vizinhos

MAC spoofing: usurpar MAC address

- Quando o sniff nos revela o MAC address de uma máquina, podemos usurpa-lo
- Para isso, podemos configurar a nossa placa de rede para usar esse endereço
- Dessa forma, a nossa placa vai transmitir e receber informação como se fosse o alvo
- Isto é possível porque não existe qualquer tipo de autenticação ao nível da camada lógica

Camada de rede (IP)

Não existe autenticação

- Podemos enviar pacotes a quem quisermos:
  - scanning
    - detetar máquinas na rede
    - enviar mensagens e observar respostas para caracterizar alvo potencial, detetar vulnerabilidades, etc.
  - DoS
    - sobrecarregar alvo com mais mensagens do que as que consegue tratar

ARP poisoning/spoofing: usurpar IP

- O protocolo ARP permite traduzir endereços IP em endereços MAC
    - Quando uma máquina não sabe qual é o endereço MAC de outra com quem quer comunicar, pode fazer um pedido ARP indicando o IP com quem pretende comunicar
    - Se a máquina alvo estiver à escuta, responde com o seu IP e indica o seu endereço MAC
- O facto de as máquinas e os switch fazerem cache desta informação permite usurpar IPs
    - Inunda-se a rede com respostas ARP em que se associa o nosso MAC address aos IPs que nos interessam
- Permite fazer attacker Man in the Middle:
    - convence-se nós legítimos que a nossa máquina possui o IP do interlocutor
    - isso implica que os pacotes são enviados para o nosso MAC address
    - lemos/processamos as mensagens e depois enviamos para o MAC address correcto

Hijacking de routing

- ICMP Router Discovery Protocol (IRDP) permite a descoberta de um router na rede
- IRDP spoofing => anunciar um router falso:
  - o atacante faz com que as máquinas nessa subnet passem a utilizar como router uma máquina controlada pelo atacante
- Informação de routing não autenticada: ao nível do BGP é possível contaminar as tabelas e redirecionar tráfego

In February 2013, we observed a sequence of events, lasting from just a few minutes to several hours in duration, in which global traffic was redirected to Belarusian ISP GlobalOneBel. These redirections took place on an almost daily basis throughout February, with the set of victim networks changing daily. Victims whose traffic was diverted varied by day, and included major financial institutions, governments, and network service providers. Affected countries included the US, South Korea, Germany, the Czech Republic, Lithuania, Libya, and Iran.

https://www.internetsociety.org/blog/2014/02/bgp-hijacking-in-iceland-and-belarus-shows-increased-need-for-bgp-security/

Rogue DHCP

- O protocolo DHCP funciona da seguinte forma
  - O cliente faz um anúncio de que precisa de um IP
  - O servidor responde com uma proposta de endereço IP (podem haver vários servidores a oferecer várias propostas)
  - O cliente pede directamente ao servidor DHCP o endereço IP
  - O servidor responde com um acknowledgement
  - Quando existem várias sub-redes, um agente DHCP pode servir de intermediário para falar com o servidor DHCP
- Um rogue DHCP server pode convencer um cliente de que o router/gateway está num IP controlado pelo adversário, permitindo um ataque Man in the Middle

Domain Name Service (DNS)

- Nada é autenticado
  (por regra não se usa DNSSEC):
  - é possível sermos direcionados para máquina diferente
- Imperativo usar autenticação da máquina relativamente a nome de domínio:
  - E.g. lembrar proteções web baseadas em origem
  - E.g. lembrar ataques man in the middle

List of Root Servers

HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

https://www.iana.org/domains/root/servers

DNS spoofing

- Convencer o alvo que que o servidor DNS é uma máquina controlada pelo atacante, isso permite
  - Fornecer endereços IP falsos, para máquinas controladas pelo atacante
  - Para enganar os utilizadores apresentando-lhes serviços credíveis
  - E extrair informação sensível, e.g., passwords
- O primeiro passo (usurpar o DNS) pode ser efectuado directamente na máquina do alvo, e.g. através de malware, ou com técnicas anteriores de usurpação de IPs
  - E.g., pode usar-se um servidor DHCP malicioso, um router malicioso, etc.

DNS (cache) poisoning

- Conhecido como Kaminsky Attack
  - Bombardear servidor DNS local com respostas de resolução DNS
  - Faz-se brute-force aos parâmetros desconhecidos na pergunta DNS (query ID)
  - Servidor DNS local aceita resposta que contém IP controlado pelo atacante
  - Servidor DNS local informa máquina do utilizador com IP errado
- Impacto aumenta com o caching de endereços resolvidos

https://en.wikipedia.org/wiki/Dan_Kaminsky

(U) New Hotness

- (TS//SI//REL) QUANTUMBISCUIT
  - Redirection based on keywork
  - Mostly HTML Cookie Values
- (TS//SI//REL) QUANTUMDNS
  - DNS Hijacking
  - Caching Nameservers
- (TS//SI//REL) QUANTUMBOT2
  - Combination of Q-BOT/Q-BISCUIT for web based Command and controlled botnets