

# Network Management

## Säkerhet

Emma Fitzgerald



# Zoom Says Investigating Problems With Videoconferencing Service in China

By Shai Oster · 18 days ago · Source: The Information

Zoom Vide  
online vid  
its users w

## Azure global outage: Our DNS update mangled domain records, says Microsoft

The compa Azure, Microsoft 365, Dynamics, Power BI, DevOps, all down for nearly two hours.

[Log in](#) | [Sign up](#) | [Forums](#) | [Serverless](#) | [M<sup>3</sup>](#) | [CLL](#) | [Webcasts](#) | [Whitepapers](#) | [The Next](#)



[DATA CENTRE](#) | [SOFTWARE](#) | [SECURITY](#) | [DEVOPS](#) | [BUSINESS](#) | [PERSONAL TECH](#)  
[SCIENCE](#) | [EMERGENT TECH](#) | [BOOTNOTES](#) | [LECTURES](#) 🔍

Data Centre ▶ **Cloud**

**Yahoo! customers! wake! up! to!  
borked! email! (Yes! people! still!  
actually! use! it!)**

FFS!

By [Richard Speed](#) 5 Sep 2019 at 09:41

### Most read



The D in Systemd is for Directories: Poettering says his creation will phone /home in future

Download Now

RECOMMENDED FOR YOU

id: Deployment, dr  
and value

provided by TechRe

# Nättjänster

DNS (drift, delegeringar)

central mail-service

- ◆ utgående mail (SMTP-server)
- ◆ inkommande mail (mailboxes, tjänster för hämtning)

IP-adresstilldelning

- ◆ manuellt (adressallokering)
- ◆ DHCP, bootp (service)

# SNMP

GET request

GET response

SET request

TRAP

MIB

- ◆ Management Information Base

# Felsökning

”Att mäta är att veta”

ping

- ◆ icmp echo

tracert

avlyssning (sniffning)

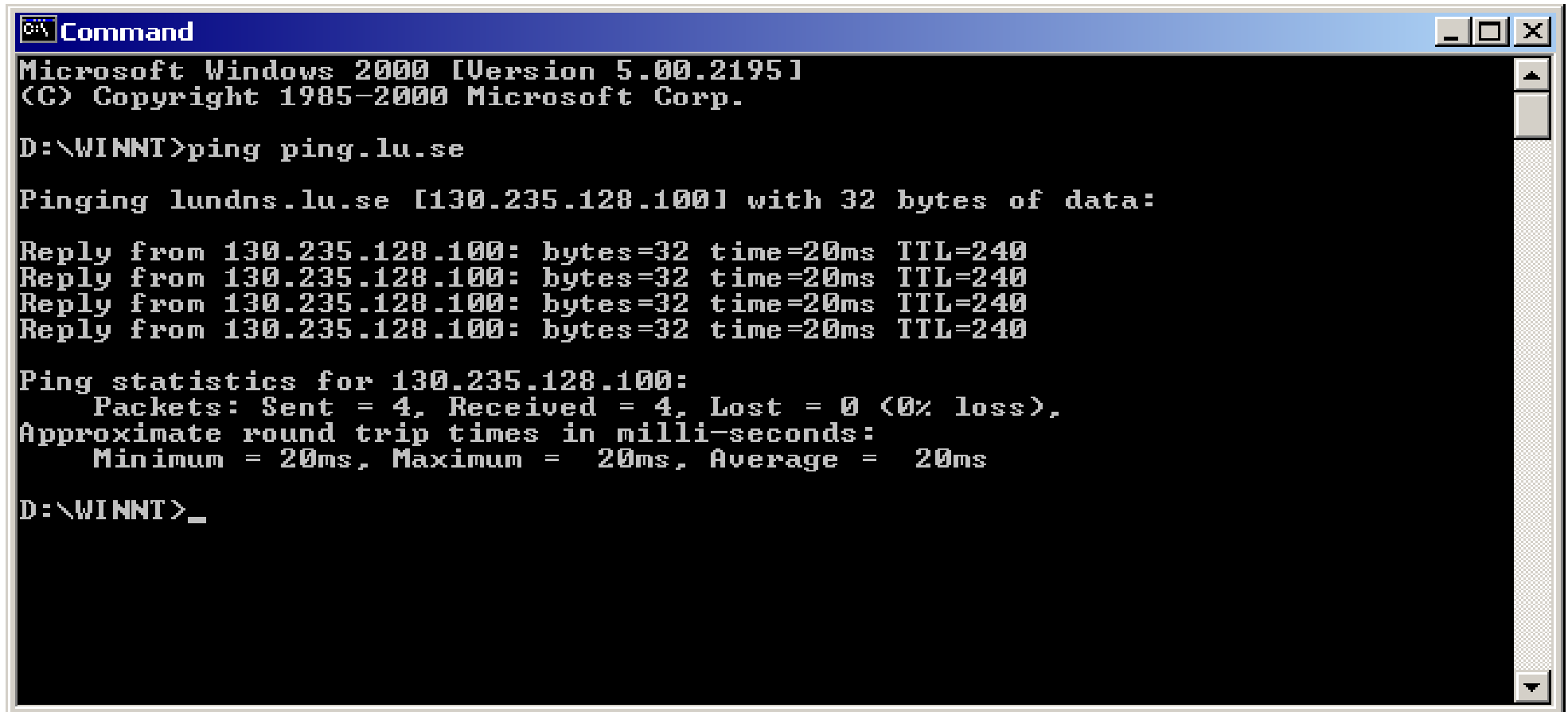
loggar

# ICMP

## Hjälpprotokoll till IP Meddelanden

- ◆ Felmeddelanden
  - Host unreachable
  - Net unreachable
  - TTL expired
- ◆ Förfrågningar
  - Echo request

# ping = icmp echo



```
Command
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

D:\WINNT>ping ping.lu.se

Pinging lundns.lu.se [130.235.128.100] with 32 bytes of data:

Reply from 130.235.128.100: bytes=32 time=20ms TTL=240
Reply from 130.235.128.100: bytes=32 time=20ms TTL=240
Reply from 130.235.128.100: bytes=32 time=20ms TTL=240
Reply from 130.235.128.100: bytes=32 time=20ms TTL=240

Ping statistics for 130.235.128.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 20ms, Average = 20ms

D:\WINNT>_
```

# traceroute

```
Command
D:\WINNT>
D:\WINNT>
D:\WINNT>
D:\WINNT>
D:\WINNT>
D:\WINNT>
D:\WINNT>
D:\WINNT>tracert ping.lu.se

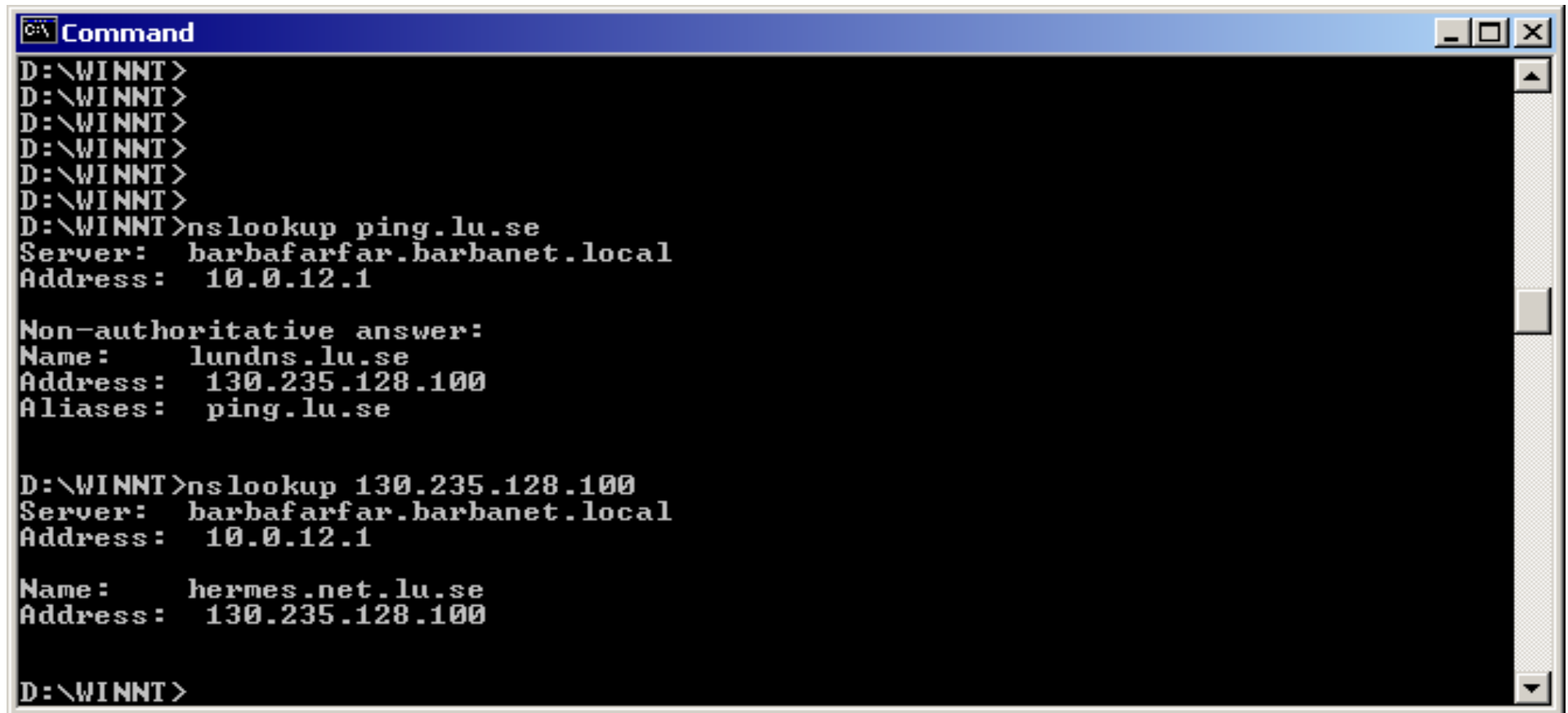
Tracing route to lundns.lu.se [130.235.128.100]
over a maximum of 30 hops:

  1  <10 ms    10 ms    <10 ms    barbafarfar.barbanet.local [10.0.12.1]
  2  <10 ms    10 ms    10 ms     gw-n1fls302o1100.telia.com [194.236.208.1]
  3  10 ms     10 ms    10 ms     10.0.111.1
  4  10 ms     10 ms    10 ms     217.211.120.187
  5  10 ms     10 ms    10 ms     m-b-c1-link.se.telia.net [81.228.72.108]
  6  10 ms     10 ms    50 ms     m-b-d1-link.se.telia.net [81.228.72.107]
  7  10 ms     10 ms    10 ms     malmo4-ge2.sunet.se [195.69.117.19]
  8  20 ms     60 ms    *         lu2-SRP1.sunet.se [130.242.85.38]
  9  20 ms     30 ms    20 ms     fys-gw-xbb ldc.lu.se [130.235.8.111]
 10  20 ms     20 ms    30 ms     hermes.net.lu.se [130.235.128.100]

Trace complete.
D:\WINNT>
```



# nslookup/host



```
C:\ Command
D:\WINNT>
D:\WINNT>
D:\WINNT>
D:\WINNT>
D:\WINNT>
D:\WINNT>
D:\WINNT>
D:\WINNT>nslookup ping.lu.se
Server:  barbafarfar.barbanet.local
Address:  10.0.12.1

Non-authoritative answer:
Name:     lundns.lu.se
Address:  130.235.128.100
Aliases:  ping.lu.se

D:\WINNT>nslookup 130.235.128.100
Server:  barbafarfar.barbanet.local
Address:  10.0.12.1

Name:     hermes.net.lu.se
Address:  130.235.128.100

D:\WINNT>
```

# Datasäkerhet?

skydd av fysisk dator- och nätutrustning

skydd av data

skydd av tillgänglighet till datasystem och applikationer

# Hur skydda dator/data?

skaffa säkerhetspolicy

använd den

följ upp den

Tänk efter vad som kan hända och motverka det!

# Brandväggar

## Packet filtering

- ◆ OSI-nivå 3 (adress-filter)

## Circuit level

- ◆ OSI-nivå 4 (jämför TCP-sessioner)

## Application level

- ◆ OSI-nivå 7 (måste känna till hur applikationen fungerar)

# Kryptering

## Symmetrisk

- ◆ Samma hemliga nyckel vid kryptering och dekryptering

## Asymmetrisk

- ◆ Öppen publik nyckel; privat hemlig nyckel

## Nyckelhantering

- ◆ Vem verifierar nycklar?
- ◆ Vem tillhandahåller nycklar?

## PGP / X.509

# Autentisering

Säkerställ motparten

Påminner om kryptering

Använd nycklar/certifikat för signering av data

# SSL

Secure Sockets Layer

Säker och autentiserad dataöverföring mellan  
webbklient och –server

https

certifikat



# TLS

- TLS = Transport Layer Security
- Vidareutveckling av SSL
- rfc 5246

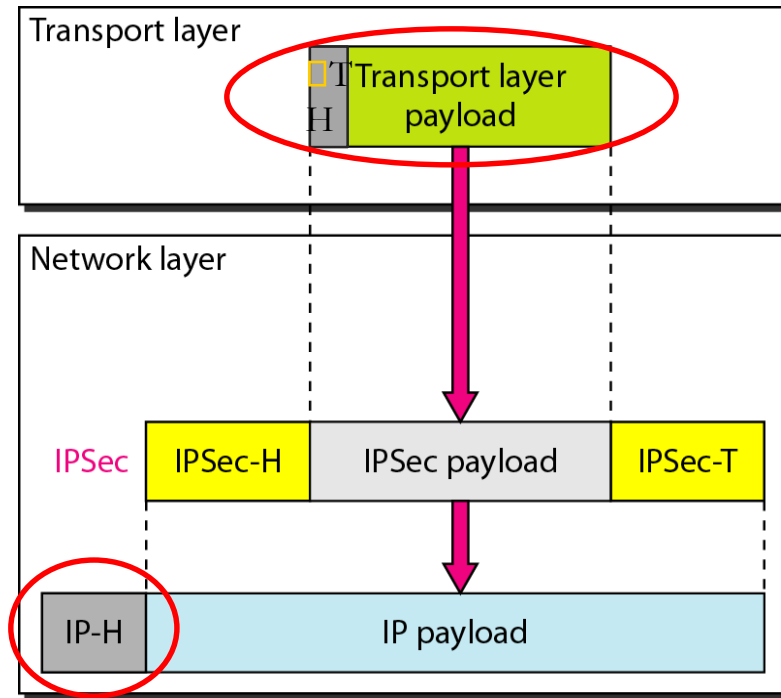


# IPsec

- IETF rfc, standard
- Tillägg till IPv4; ingår i IPv6
- Två moder
  - ◆ Transport mode
    - Signera data genom att lägga till Ipsec-header
  - ◆ Tunnel mode
    - Kryptera ip-paket; kapsla in i annat ip-paket mellan tunnelns ändpunkter

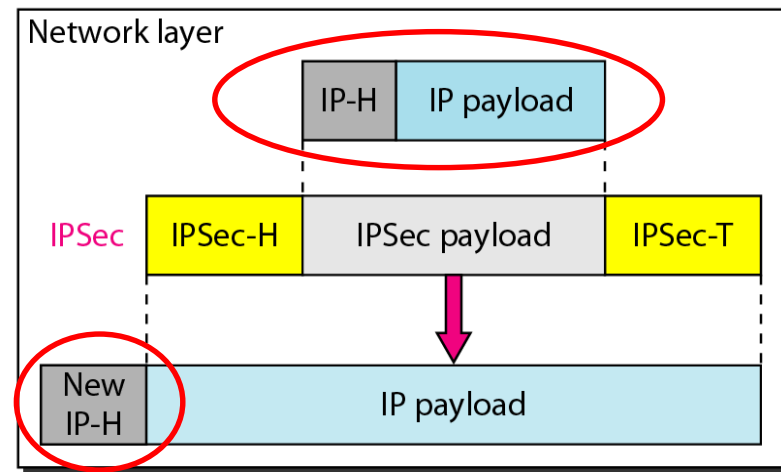
# IPSec

## *Transport mode*



a. Transport mode

## *Tunnel mode*



b. Tunnel mode

# Andra säkerhetsprotokoll

- WEP
  - Wire Equivalent Privacy
  - **Inte alls säkert**
- WPA/WPA2
  - WiFi Protected Access
  - WPA2 = IEEE 802.11i

# Hur skydda dator/data?

**BACKUP. Ofta!**

**Antivirusprogram. Uppdatera!**

**Öppna ALDRIG attachments om du inte vet vad de innehåller.**

**Gå endast till kända web-sidor. Följ inte kryptiska länkar.**

**Personlig brandvägg!!!!**

**Kryptera data.**