

**FIT9137**

# **Introduction to Computer Architecture and Networks**

**Week 11: Workshop on Virtual Private Network (VPN)  
& Digital Inclusion**

Safi Uddin



www.shutterstock.com • 1322202464

# SETU Feedback

**We appreciate your feedback!**

# Learning Outcomes

- **Properly identify the security and privacy threats in a network environment**
- Understand security enabling techniques
- **Appropriately implement VPN services**

# Virtual Private Networks

# Virtual Private Networks

## **Virtual Private Networks - VPN**

- establishes a secure, encrypted connection between your computer and the internet.
- creates a private tunnel for your data communications over public networks

# Virtual Private Networks

Use **Internet** as the Packet Switched Network

- easily available
- low cost due to lots of competition
- flexible

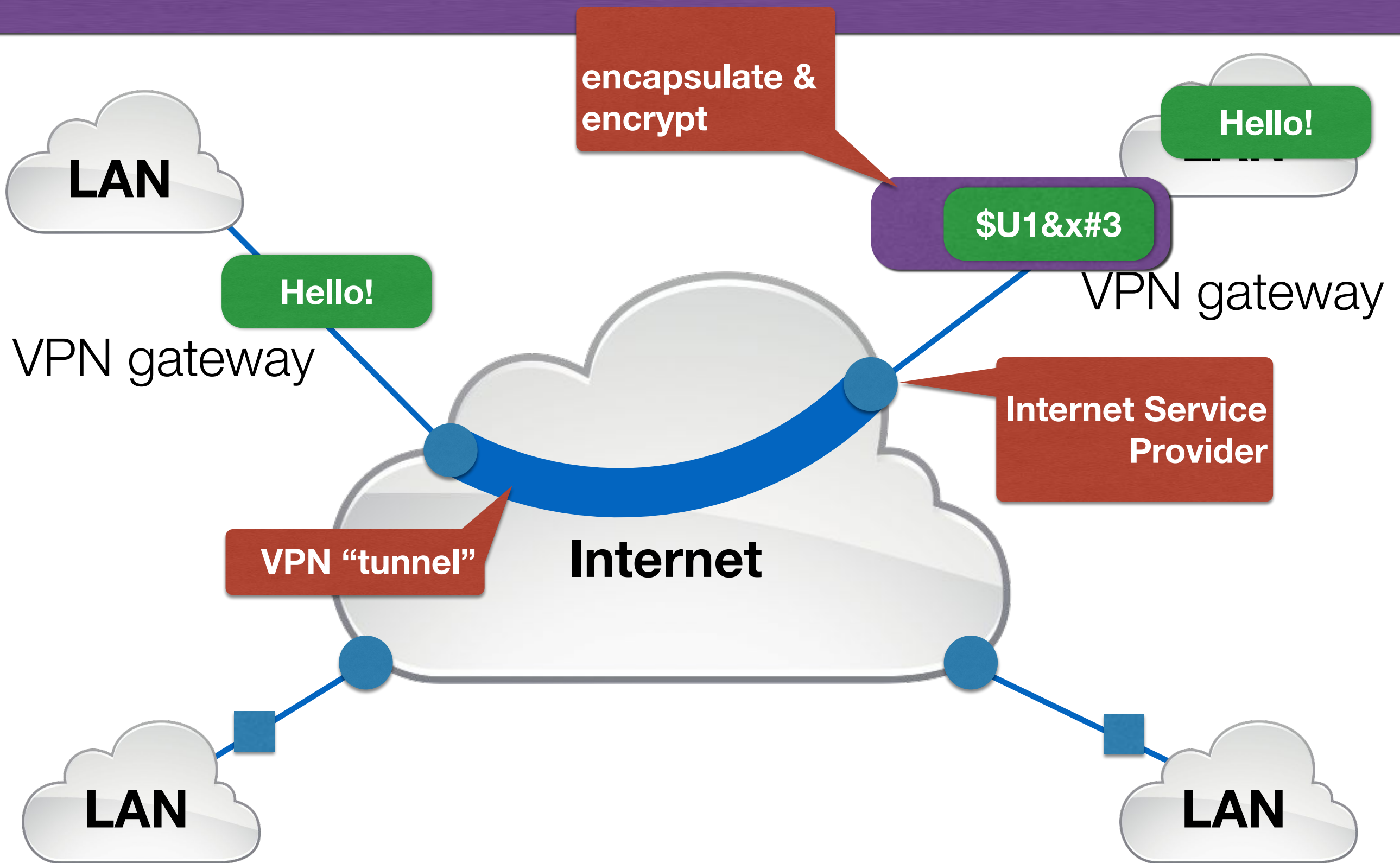
How does it work?

- software simulates “virtual NIC”
- packets are **encapsulated**, then sent through Internet
- receiver unpacks, then sends into LAN

Note: nothing to do with Virtual LAN!



# Virtual Private Networks



# Types of VPNs

## Intranet VPN

- connect LANs of the **same** organization
- uses special VPN gateway devices

## Extranet VPN

- connect **different** organizations (e.g., a company with its customers)
- same technology as intranet

## Access VPN

- allows employees to access company intranet over the Internet
- uses special gateway at the company + simple client software for the employees
- Monash offers an Access VPN

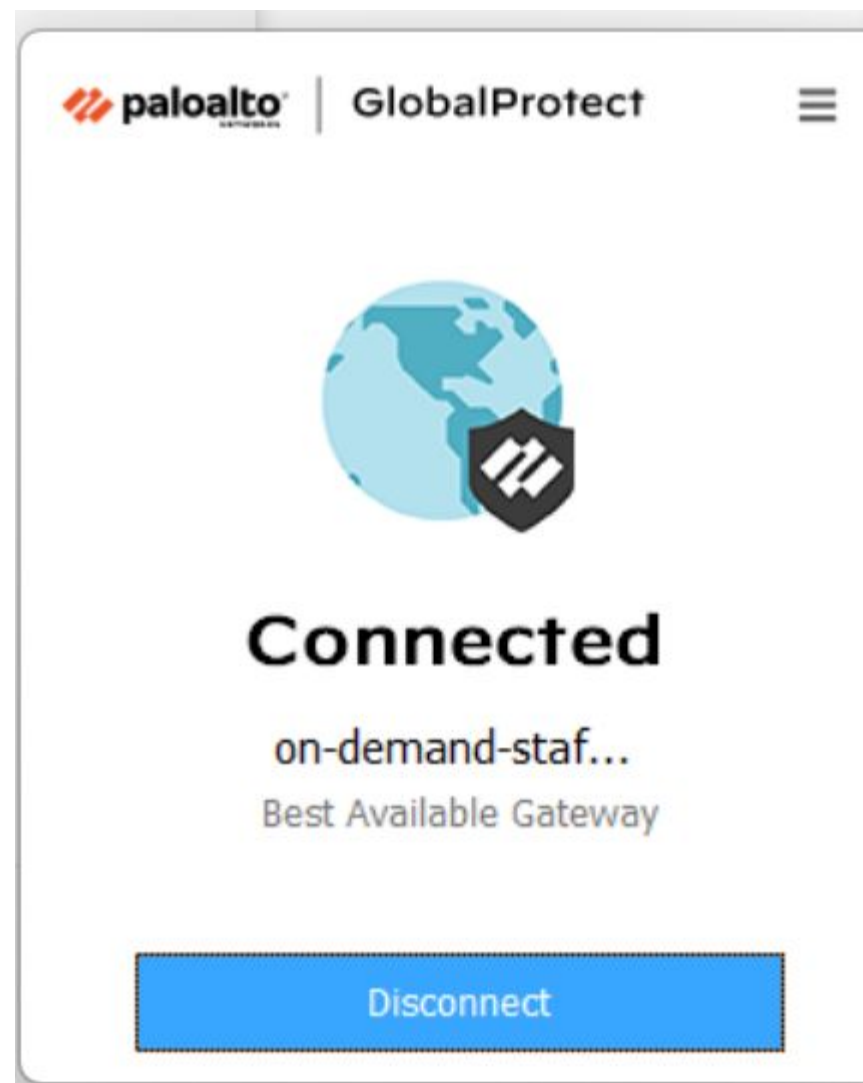


# Using the Monash VPN

## **Example: access library resources**

- Monash has subscriptions to many online journals
- access is restricted to Monash IPs: 130.194.X.X
- using VPN, you get a Monash IP!

# VPN using GlobalProtect



# VPN

## Advantages

Low cost

Easy setup

Secure

Flexible (endpoints can move)

## Disadvantages

No performance guarantees

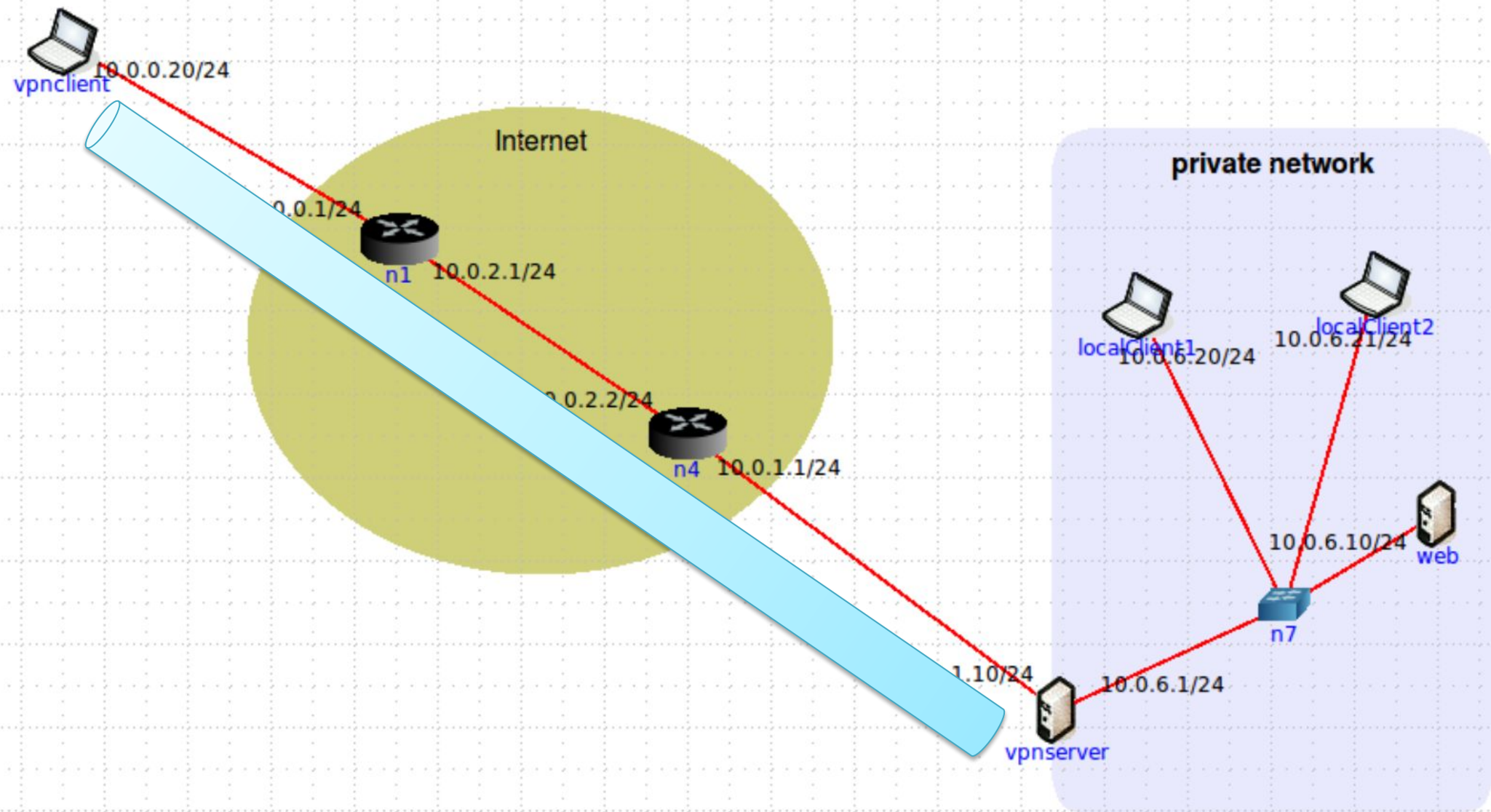
Introduces overhead (encryption, encapsulation)

Many incompatible standards

# Activity A

# VPN

## External Network – Home Network





# • ACTIVITY A: VPN

We will use the core file [FIT9137\\_Week-11\\_Activity\\_VPN.imn](#). Open the file in CORE inside VM. The configuration contains a network design with a private network on the right, some public (Internet) routers in the middle, and a client in the top left that wants to connect to the private network. Start the emulation and perform the following tasks: `lynx 10.0.6.10`

**STEP-1.** See if you can reach the devices inside the private network. You can for instance ping the clients or run `lynx` with the address of the server. Run a traceroute between `vpnclient` and `web`. What do you see?

```
LXTerminal
File Edit Tabs Help
root@vpnclient:/tmp/pycore.34300/vpnclient.conf# cd ~
root@vpnclient:/root#
root@vpnclient:/root#
root@vpnclient:/root# ping 10.0.6.10
PING 10.0.6.10 (10.0.6.10) 56(84) bytes of data.
64 bytes from 10.0.6.10: icmp_seq=1 ttl=63 time=0.561 ms
64 bytes from 10.0.6.10: icmp_seq=2 ttl=63 time=0.991 ms
64 bytes from 10.0.6.10: icmp_seq=3 ttl=63 time=0.452 ms
^C
--- 10.0.6.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2147ms
rtt min/avg/max/mdev = 0.452/0.668/0.991/0.232 ms
root@vpnclient:/root# traceroute 10.0.6.10
traceroute to 10.0.6.10 (10.0.6.10), 64 hops max
 1  10.0.200.1  0.448ms  0.328ms  0.357ms
 2  10.0.6.10  0.330ms  0.326ms  0.243ms
root@vpnclient:/root#
```

1

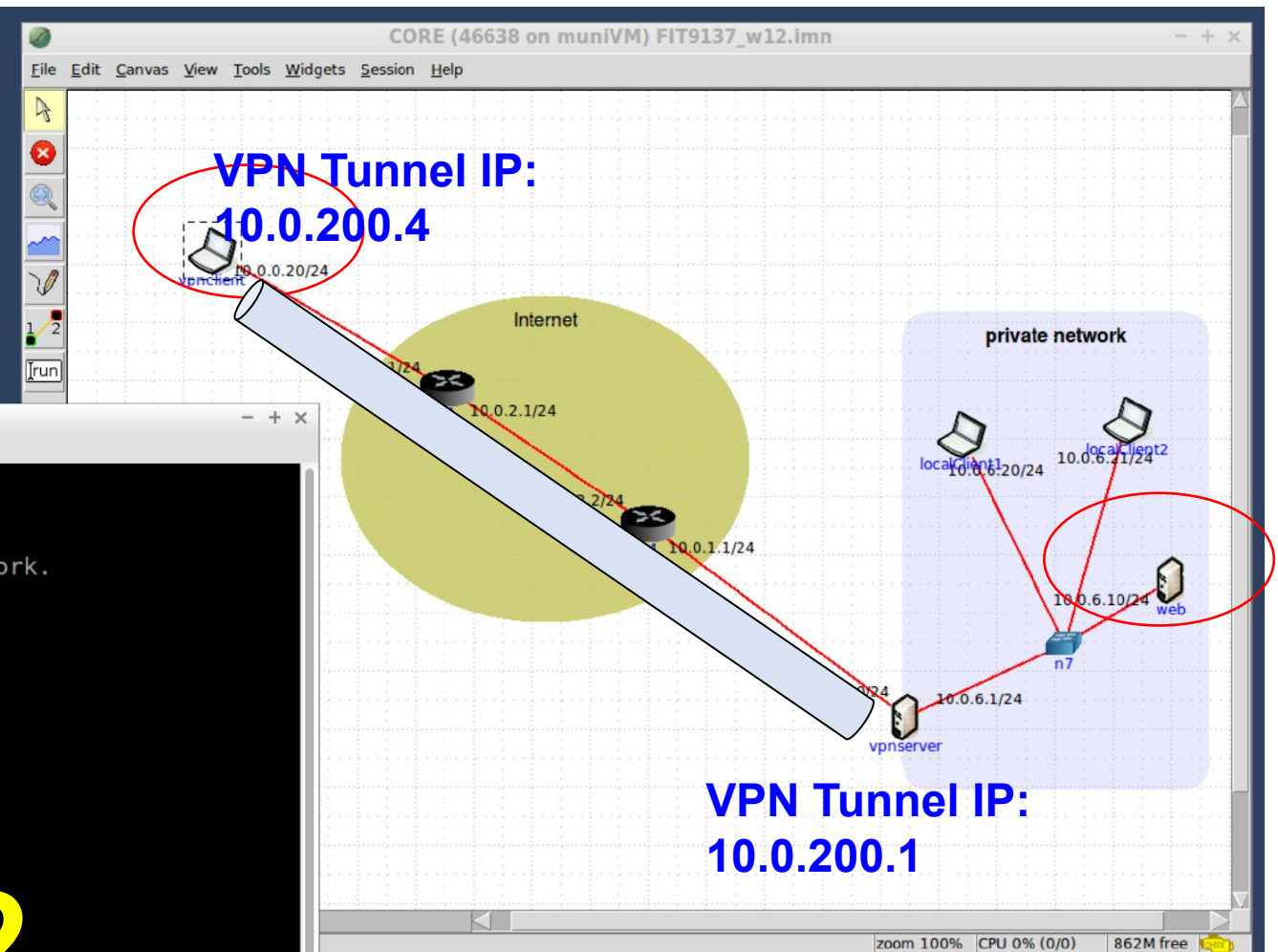
```
root@vpnclient: ~
File Edit Tabs Help

VPN internal web server

This web server is located inside a virtual private network.

Commands: Use arrow keys to move, '?' for help, 'q' to quit, '<-' to go back.
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

2





# • ACTIVITY A: VPN

STEP-2. Run *ifconfig* for checking local network interfaces we find the tun0 interface:?

The image shows a network diagram and a terminal window. The diagram, titled "CORE (46638 on muniVM) FIT9137\_w12.imn", illustrates a VPN setup. It features an "Internet" cloud and a "private network" cloud. A "vpnclient" is connected to the Internet. A "vpnserver" is connected to the private network. The VPN Tunnel IP for the client is 10.0.200.4, and for the server is 10.0.200.1. The diagram also shows various network interfaces and their IP addresses, such as n1 (10.0.0.1/24), n4 (10.0.2.2/24), n7 (10.0.6.10/24), and web (10.0.6.1/24). The terminal window, titled "root@vpnclient: ~", displays the output of the *ifconfig* command for the *tun0* interface. The output shows that the interface is up and running, with a link encap of UNSPEC and a hardware address of 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00. The IP address is 10.0.200.4, and the mask is 255.255.255.255. The interface is also configured with a point-to-point link and a metric of 1.

```
root@vpnclient: ~  
File Edit Tabs Help  
TX packets:119 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:17034 (17.0 KB) TX bytes:14916 (14.9 KB)  
  
lo Link encap:Local Loopback  
inet addr:127.0.0.1 Mask:255.0.0.0  
inet6 addr: ::1/128 Scope:Host  
UP LOOPBACK RUNNING MTU:65536 Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
tun0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  
-00  
inet addr:10.0.200.4 P-t-P:10.0.200.1 Mask:255.255.255.255  
inet6 addr: fe80::4b8a:44b:baf4:308d/64 Scope:Link  
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1  
RX packets:11 errors:0 dropped:0 overruns:0 frame:0  
TX packets:19 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:100  
RX bytes:1052 (1.0 KB) TX bytes:1127 (1.1 KB)  
  
root@vpnclient:~#
```

# • ACTIVITY A: VPN

STEP-3. Run Wireshark on one of the routers. Then **run lynx again from vpnclient accessing web** or **ping webServer**. Can you see the HTTP protocol messages or the ICMP echo request and replies?

The screenshot displays a network simulation environment with three main components:

- Terminal Window (root@vpnclient: ~):** Shows the output of a ping command to 10.0.6.10. The statistics indicate 20 packets transmitted, 20 received, 0% packet loss, and a time of 19403ms. The output shows ICMP echo request and reply details.
- Wireshark Window (\*veth1.0.98):** Displays a list of captured packets. The selected packet is an OpenVPN message (P\_DATA\_V1) with a length of 175 bytes. The packet details show the OpenVPN protocol and the message type.
- Network Diagram (CORE (46638 on muniVM) FIT9137\_w12.imn):** Illustrates the network topology. It shows the Internet (yellow circle), a private network (blue circle), and a VPN tunnel (blue cylinder). The VPN tunnel connects the private network to the Internet. The diagram includes labels for various network elements: n1, n4, n7, localClient1, localClient2, and web. The VPN Tunnel IP is highlighted as 10.0.200.4 and 10.0.200.1.



# • ACTIVITY A: VPN

STEP-4. Run Wireshark on the interface eth1 (with IP 10.0.6.1) of the vpnserver. Run lynx as before. What can you see in the captured traffic?

The screenshot displays a virtual machine environment with three main components:

- Wireshark Window (\*veth5.1.98):** Shows a packet capture on interface eth1. The capture list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.200.4	10.0.6.10	TCP	74	41690 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1353 SACK PER
2	0.000041040	10.0.6.10	10.0.200.4	TCP	74	80 → 41690 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=14
3	0.000224592	10.0.200.4	10.0.6.10	TCP	66	41690 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=42692
4	0.000785528	10.0.200.4	10.0.6.10	HTTP	319	GET / HTTP/1.0
5	0.000824098	10.0.6.10	10.0.200.4	TCP	66	80 → 41690 [ACK] Seq=1 Ack=254 Win=65024 Len=0 TSval=247
6	0.001295595	10.0.6.10	10.0.200.4	HTTP	460	HTTP/1.1 200 OK
7	0.001428924	10.0.6.10	10.0.200.4	TCP	66	80 → 41690 [FIN, ACK] Seq=395 Ack=254 Win=65024 Len=0 TS
8	0.001612198	10.0.200.4	10.0.6.10	TCP	66	41690 → 80 [ACK] Seq=254 Ack=395 Win=64128 Len=0 TSval=4
9	0.002461315	10.0.200.4	10.0.6.10	TCP	66	41690 → 80 [FIN, ACK] Seq=254 Ack=396 Win=64128 Len=0 TS
10	0.002494383	10.0.6.10	10.0.200.4	TCP	66	80 → 41690 [ACK] Seq=396 Ack=255 Win=65024 Len=0 TSval=2

- Network Diagram:** Illustrates the VPN setup. A yellow circle represents the 'Internet'. A blue cylinder represents the 'VPN Tunnel'. A blue circle represents the 'private network'. The tunnel connects the Internet to the private network. The tunnel's IP is 10.0.200.1 (labeled 'VPN Tunnel IP: 10.0.200.1'). The private network contains a 'web' server (IP 10.0.6.10/24) and two 'local client' machines (IPs 10.0.6.1/24 and 10.0.6.2/24). The tunnel's other end is labeled 'VPN Tunnel IP: 10.0.200.4'. The private network is also labeled 'private network'.
- Terminal Window (root@vpnclient: ~):** Shows the output of the 'lynx' command, displaying a web page titled 'VPN internal web server'. The page content is: 'This web server is located inside a virtual private network.' The terminal also shows the command prompt and the output of the 'lynx' command.

# • ACTIVITY A: VPN

STEP-5. Check the file client.conf on vpnclient and server.conf on vpnserver and use openvpn manual (man openvpn) to learn more about the settings. For instance, what encryption algorithm is used, what key exchange algorithm is used, what are the client and server key pairs etc.

The image displays a network diagram and two terminal windows. The diagram, titled 'CORE (46686 on muniVM) FIT9137\_w12.imn', shows a central 'Internet' cloud connected to a router 'n1' (10.0.0.1/24). A 'vpnclient' (10.0.0.20/24) is connected to the router. The router is also connected to a 'private network' (10.0.6.0/24) containing 'local client1' (10.0.6.20/24) and 'local client2' (10.0.6.21/24). Below the diagram are two terminal windows. The left terminal, titled 'LXTerminal', shows the contents of 'client.conf' on the 'vpnclient' machine. The right terminal, also titled 'LXTerminal', shows the contents of 'server.conf' on the 'vpnserver' machine.

**Vpnclient: client.conf**

```
root@vpnclient:/tmp/pycore.46686/vpnclient.conf# ls
client.conf  var.log  vpnclient.key  vpnclient.pem
defaultroute.sh  var.run  vpnclient.log  vpnclient.sh
root@vpnclient:/tmp/pycore.46686/vpnclient.conf# cat client.conf
client
dev tun
proto udp
remote 10.0.1.10 1194
nobind
ca /tmp/pycore.46686/certs/ca-cert.pem
cert /tmp/pycore.46686/vpnclient.conf/vpnclient.pem
key /tmp/pycore.46686/vpnclient.conf/vpnclient.key
dh /tmp/pycore.46686/certs/dh2048.pem
cipher AES-256-CBC
log /var/log/openvpn-client.log
verb 4
daemon
root@vpnclient:/tmp/pycore.46686/vpnclient.conf#
```

**vpnserver: server.conf**

```
etc.ssh  server.conf  var.run  vpnserver.log
ipforward.sh  startsshd.sh  var.run.sshd  vpnserver.pem
root@vpnserver:/tmp/pycore.46686/vpnserver.conf# cat server.conf
# openvpn server config
local 10.0.1.10
server 10.0.200.0 255.255.255.0
push redirect-gateway def1
push route 10.0.6.0 255.255.255.0
keepalive 10 120
ca /tmp/pycore.46686/certs/ca-cert.pem
cert /tmp/pycore.46686/vpnserver.conf/vpnserver.pem
key /tmp/pycore.46686/vpnserver.conf/vpnserver.key
dh /tmp/pycore.46686/certs/dh2048.pem
cipher AES-256-CBC
status /var/log/openvpn-status.log
log /var/log/openvpn-server.log
ifconfig-pool-linear
ifconfig-pool-persist /tmp/pycore.46686/vpnserver.conf/ippool.txt
port 1194
proto udp
dev tun
verb 4
daemon
root@vpnserver:/tmp/pycore.46686/vpnserver.conf#
```

**600** hours of video uploaded to YouTube every minute

**1.75** billion daily active users on Facebook

**225** exabyte of worldwide Internet traffic per month

**5.0** trillion US\$ in online sales expected in 2023



# Mornington Island





# PollEv Question: Indigenous Peoples

Which of the following is/are true about Indigenous Peoples/Cultures in Australia:

- A. The Aboriginal and Torres Strait Islander people of Australia are **the oldest continuous civilisation on earth**, extending back over **65,000 years**.
- B. They could become Australian Citizens from the very beginning
- C. Aboriginal and Torres Strait Islander art is among the **oldest forms of art in the world**
- D. There are **less than 100,000** Indigenous People in Australia

# Activity B

# Activity Steps

## **Problem: How to provide proper Internet access to remote Indigenous communities**

1. Form groups of 5-8 students
2. Pick a “cool” group name and a representative
3. Read the two main articles (and more as you like)
4. Discuss potential issues (financial, technical, cultural, etc) around the problem
5. Come up with solutions to the problem
6. Bring something from your own cultural, educational, professional background
7. Report the following in PollEv:
  - a. Your group name
  - b. List of issues identified (with brief explanations)
  - c. Proposed solutions
  - d. Input from your own background

# Activity: Digital Inclusion

## Resources

- <https://theconversation.com/for-remote-aboriginal-families-limited-phone-and-internet-services-make-life-hard-heres-what-they-told-us-201295>
- <https://www.creativespirits.info/aboriginalculture/economy/internet-access-in-aboriginal-communities>

## Additional resources

- <https://www.niaa.gov.au/sites/default/files/documents/publications/indigenous-digital-inclusion-plan-discussion-paper.pdf>
- [https://researchbank.swinburne.edu.au/file/a67b7e2c-0717-4974-8c98-06730bd91426/1/PDF%20\(Accepted%20manuscript\).pdf](https://researchbank.swinburne.edu.au/file/a67b7e2c-0717-4974-8c98-06730bd91426/1/PDF%20(Accepted%20manuscript).pdf)

# Sample Answer

- Group name
- List of potential issues
  - Issue 1, brief explanation
  - Issue 2, brief explanation
- List of proposed solutions issues
  - Solution 1, brief explanation
  - Solution 2, brief explanation
- Individual 1's personal input
- Individual 2's personal input
- ...

internet connectivity. • Issue 2: High costs and affordability Many Aboriginal families in remote communities cannot afford internet plans or digital devices, even when services are technically available. • Issue 3: Lack of culturally appropriate digital content Most online content is not available in Aboriginal languages or aligned with cultural contexts, reducing its relevance and usability. • Issue 4: Digital literacy and training gaps There is a lack of digital skills and confidence, especially among older generations and those with limited literacy.

List of proposed solution issues

- Solution 1: Satellite and community-based Wi-Fi Deploy satellite internet services (e.g. Starlink) and establish free or low-cost Wi-Fi hubs at community centres to provide stable access in remote areas.
- Solution 2: Government-subsidised access and devices Introduce affordable internet plans and device subsidies to lower entry barriers and encourage long-term usage.
- Solution 3: Local content development Support the creation of digital resources in Aboriginal languages and cultural contexts, focusing on education, health, and local services.
- Solution 4: Digital education and local tech support Train local community members as digital ambassadors who can provide hands-on support and build community-wide digital literacy.

Individual 1's personal input I believe simply installing internet infrastructure isn't enough. We need to empower local communities by training young people to become tech support and content creators, so they can both help others and find meaningful work.

Individual 2's personal input The government must listen to the voices of



Learning Hubs Establish Wi-Fi access centers in community locations with shared computers or tablets. Provide digital literacy training in local languages to improve long-term engagement and skills. Solution 3: Community-Driven Engagement

Hire and train local "digital ambassadors" to manage the technology, lead workshops, and ensure that all digital content and support are culturally appropriate and trusted by the community. 3. Personal Contributions Qianli Huang With my background in IT, I suggest implementing a local content caching system to preload educational and health resources. This would ensure access even with limited or intermittent internet connectivity. Yicheng Gao Coming from a rural area in China, I understand the consequences of digital inequality. I recommend government-subsidized digital devices for students and a centralized remote education platform to ensure equitable access. Kangsen Huang As an education major, I believe that teacher training is essential. By equipping local teachers with digital tools and strategies, we can ensure that communities benefit sustainably from improved internet access.

- Group name: CompArch student • Issue 1: Infrastructure: an indigenous Australian community, mostly living in remote areas, and it's costly to build such infrastructure, and it has the longest BEP. • Issue 2: Digital Literacy: living in remote areas means a lack of exposure to digital devices such as computers and phones. • List of proposed solutions issues • Solution 1: using a satellite-based internet connection, such as Starlink. • Solution 2: Ensure that schools in remote