SWINBURNE
UNIVERSITY OF
TECHNOLOGY

Virtual Private Networks

Lecture thirteen

Outline of Lecture

- Types of VPNs
  - remote access, intranet and extranet
- Building blocks of a VPN
  - VPN hardware and software
  - organisation’s and service provider’s security infrastructure
  - public networks
  - tunnels
- Ways of classifying VPNs
  - who implements it
  - where the endpoints are
  - its size and complexity

Learning objectives

- At the end of this lecture, students should be able to:
  - Explain what a VPN is
  - Explain the architectures and purposes of different types of VPNs
  - Describe the basic building blocks of VPNs
  - Explain the different ways of classifying VPNs

Introduction to VPNs

- Virtual Private Network
  - Makes use of publicly available networking infrastructure to provide the features of a private network
- Definition of VPN according to the IETF
  - An emulation of a private Wide Area Network (WAN) using shared or public IP facilities such as the Internet or private IP backbones
  - An extension of a private intranet across a public network (usually the Internet)
- Originally driven by low cost and wide reach of the Internet
- Recent drivers are avoiding geoblocking and concerns about privacy

Introduction to VPNs

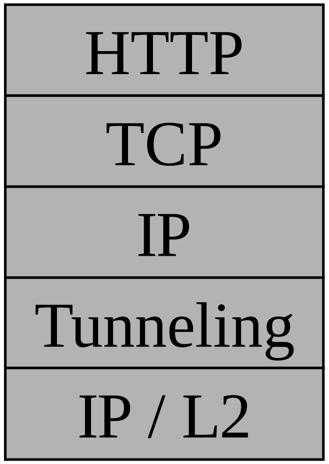
- Key concepts of VPNs are
  - Tunnels
    - Main VPN concept
    - Enables two end-points to exchange data in a way that emulates point to point communication
  - Encryption
    - Enables communication to be confidential even though using shared and very insecure Internet
  - Integrity
    - Ensures data is unchanged
  - Authorisation
    - Specifies what services and resources users can have access to

Evolution of VPNs

- VPNs are quite an old concept
  - Originally Software Defined Networks
  - developed by ATT in the late 80s
- X.25 over ISDN in the early 90s
  - Virtual circuits over shared infrastructure
  - Problems with scalability to higher bit rates
- Frame Relay mid 90s
  - Took advantage of reliability of modern media
  - Extended the idea of Virtual Circuit Switching
  - Still an important technology
- IP based VPNs late 90s

VPN Tunneling protocols

- Tunnels in VPNs
  - Encapsulate data packets in a tunneling protocol
    - Possibly other IP packets
  - Then encapsulate in IP packets or layer two frames for transmission
- Example
  - Accessing HTTP over a VPN


HTTP
TCP
IP
Tunneling
IP / L2

Tunnel used depends on the VPN type

VPN Tunneling protocols

- IP Security (IPSec)
  - IETF
  - Network layer (layer 3) protocol
- Point-to-point tunneling protocol (PPTP)
  - Obsolete (lots of security issues and other alternatives)
  - Microsoft Layer 2 protocol
- Layer 2 Tunneling Protocol (L2TP)
  - Cisco Layer 2 protocol
  - Built from L2F (layer 2 forwarding) and PPP (Point to Point Protocol)
- Secure Socket Tunnelling Protocol (SSTP)
  - Secure Sockets Layer / Transport Layer Security
  - Transport over TLS/SSL with inbuilt key exchange mechanisms

Advantages and disadvantages of VPNs

- Advantages
  - Implementation costs
  - Management costs
  - Connectivity
  - Security
  - Efficient use of network capacity
  - Scalable
  - Privacy
  - Can be used to avoid geoblocking
- Disadvantages
  - Variations in capacity
  - Reliability of the Internet

VPN Considerations

- Security
  - Essential for private traffic using the very public and insecure Internet
  - VPN security needs to be compatible with other security infrastructure
    - eg can be difficult to pass IPSec through a firewall
- Interoperability
  - Don’t want to be tied to one supplier
  - May wish to construct VPNs that span other organisations (Extranets)
- Easy to implement, manage and use
  - Particularly important that the client software is easy to implement
  - Need to keep track of potentially hundreds of tunnels

VPN Considerations

- Scalable
  - Should be able to increase number of clients and sites without modification to existing clients and sites
- Performance
  - Encryption is a resource hungry activity. Need sufficient capacity to support many encryption tunnels
  - Available bandwidth needs to be sufficient. Maybe some reservation of bandwidth is required (can be done in Frame Relay)
- Reliable ISPs
  - VPNs reliability is dependent on ISP reliability
  - May need some service level agreements

Types of VPNs

- Remote access VPNs
  - Access to mobile or telecommuting employees
  - Avoid geoblocking
- Intranet VPNs
  - Interconnect remote branch offices of an organisation
- Extranet VPNs
  - Allow controlled access to external parties
    - Customers may wish to check our inventory
    - Customers may wish to place orders
    - May wish to transfer work to and from contract organisations

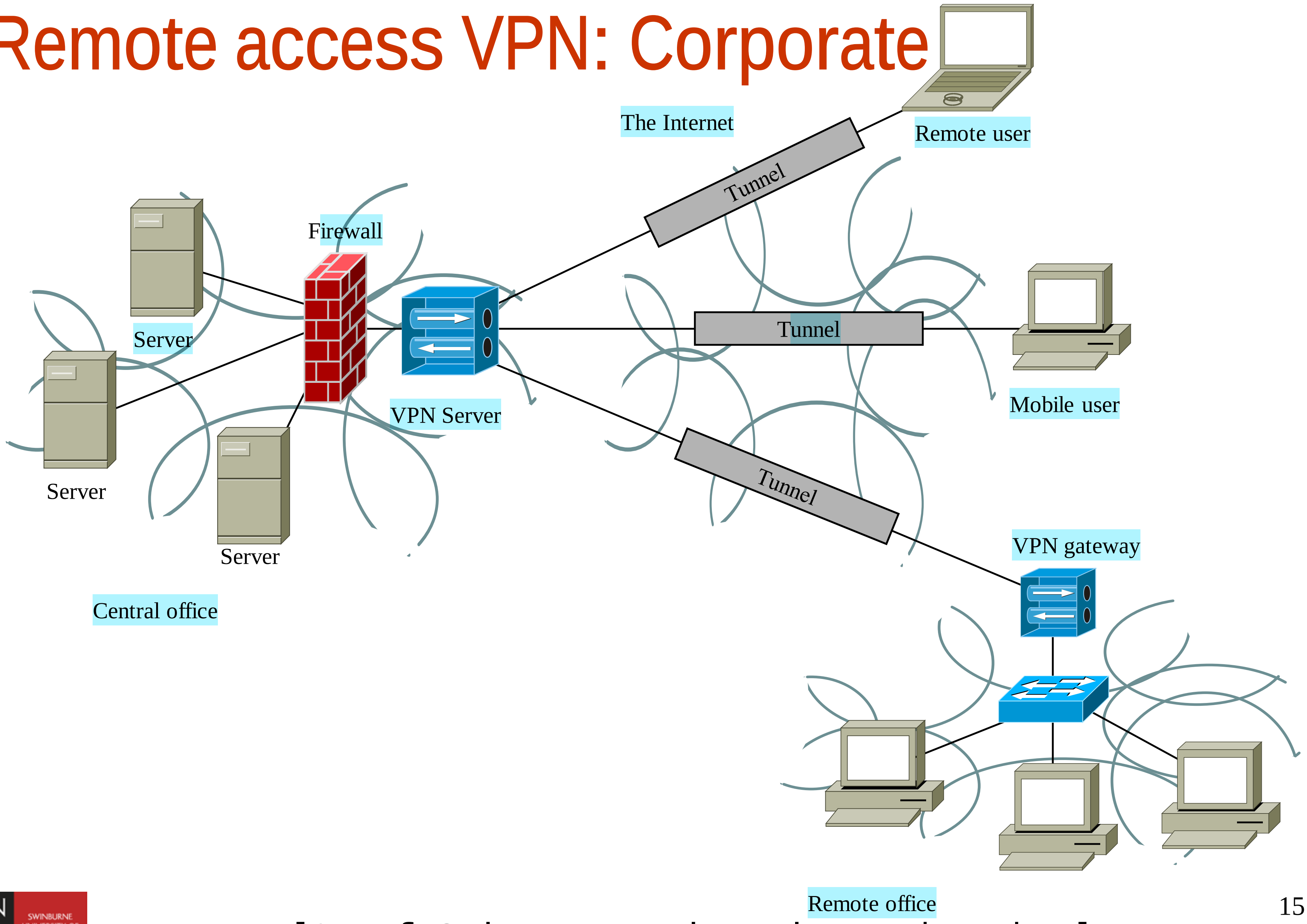
Remote access VPNs

- Typically used by mobile users and remote branches
  - sales people, frequently travelling senior managers etc
  - remote branches where a permanent connection via an Intranet is not justified
- Implemented through connection to an ISP’s nearest Point of Presence
- Single remote users and mobile users will connect via the ISP to the corporate VPN server
- Small offices may have a VPN gateway that concentrates traffic from multiple hosts
  - A switch, router or firewall appliance

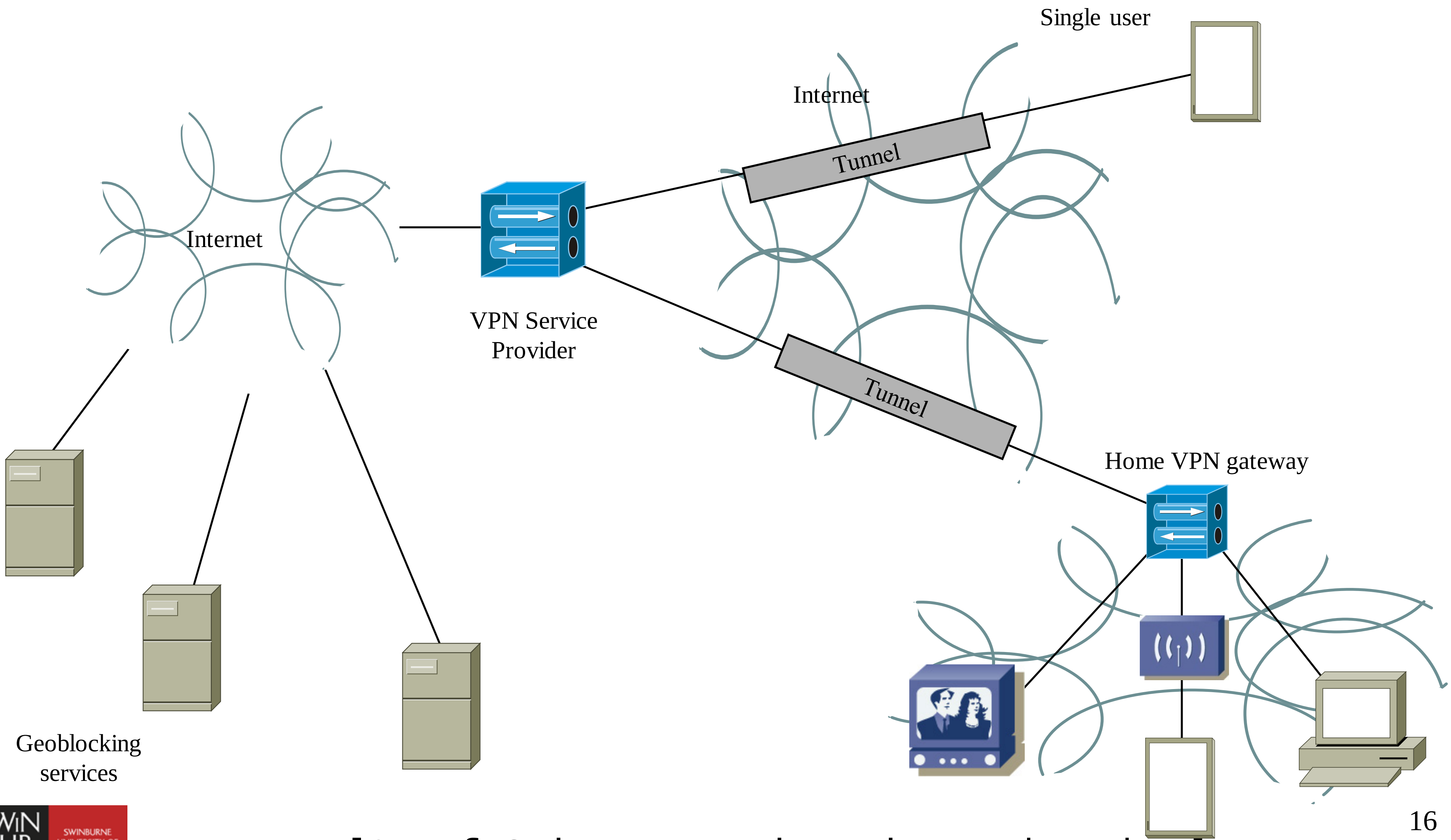
Remote Access VPNs

- The same technology can be used to avoid geoblocking or tracking of online activity
  - Typically this is household rather than office based
- Rather than connecting to a corporate VPN, the user subscribes to a VPN service located in a country which is not geoblocked
- As far as the service is concerned traffic is to and from the VPN server endpoint
- Again, there may be a shared VPN gateway (VPN client software) at the household that connects to the VPN server

Remote access VPN: Corporate



Remote access VPN: Avoiding geoblocking



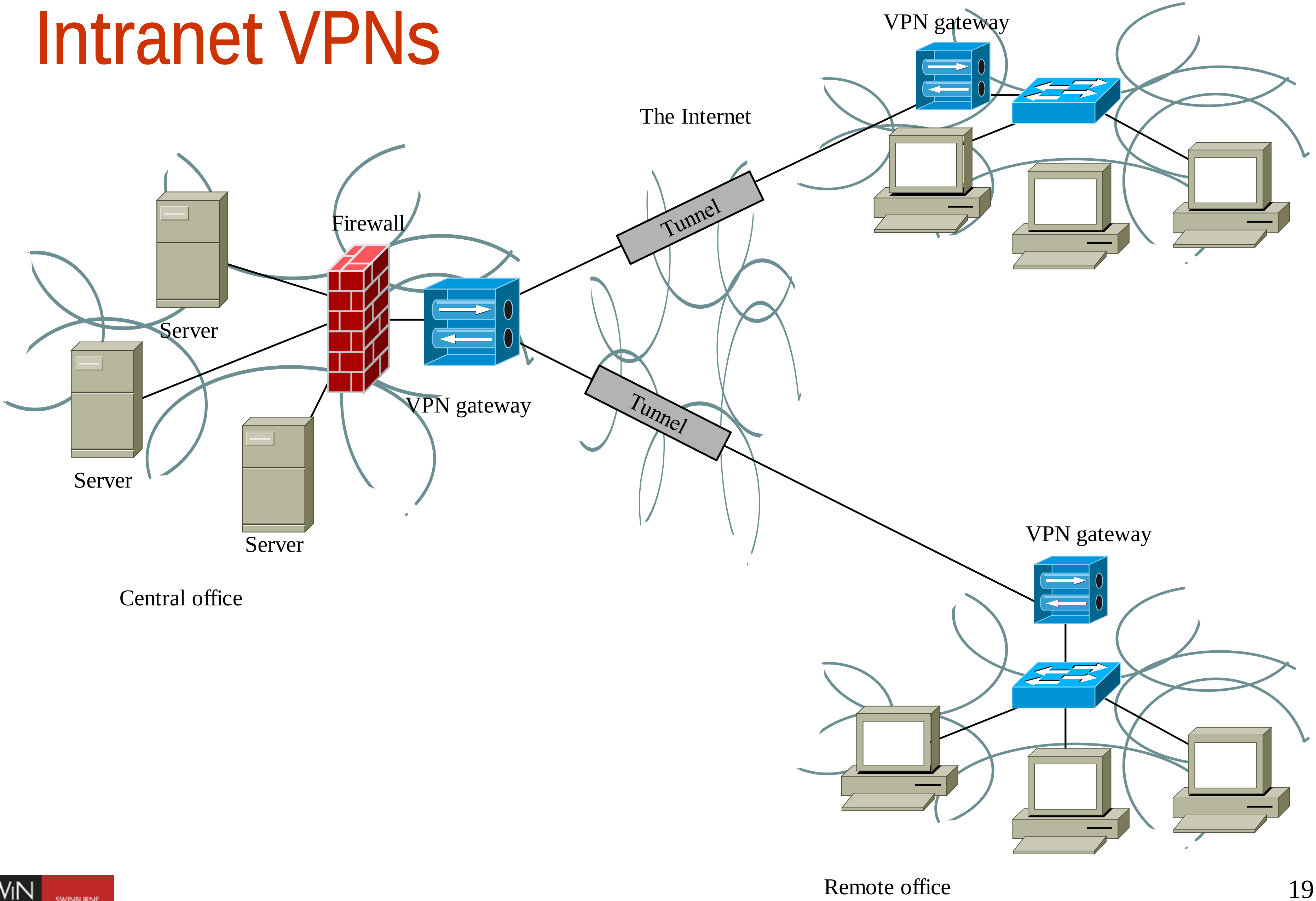
Remote access VPNs

- Advantages
  - Simple, comparatively low cost infrastructure
  - No need for support personnel at remote sites
    - Done by ISP
  - No fixed limit to number of users
    - Maybe limitations caused by performance
- Disadvantages
  - No guarantees of Quality of Service
  - Lots of protocol and computation overhead from encrypted tunnels

Intranet VPNs

- Used to interconnect remote branch offices
- Use local ISP to provide WAN connectivity rather than providing WAN connectivity directly
- Much more a peer-to-peer architecture than remote access VPNs

Intranet VPNs



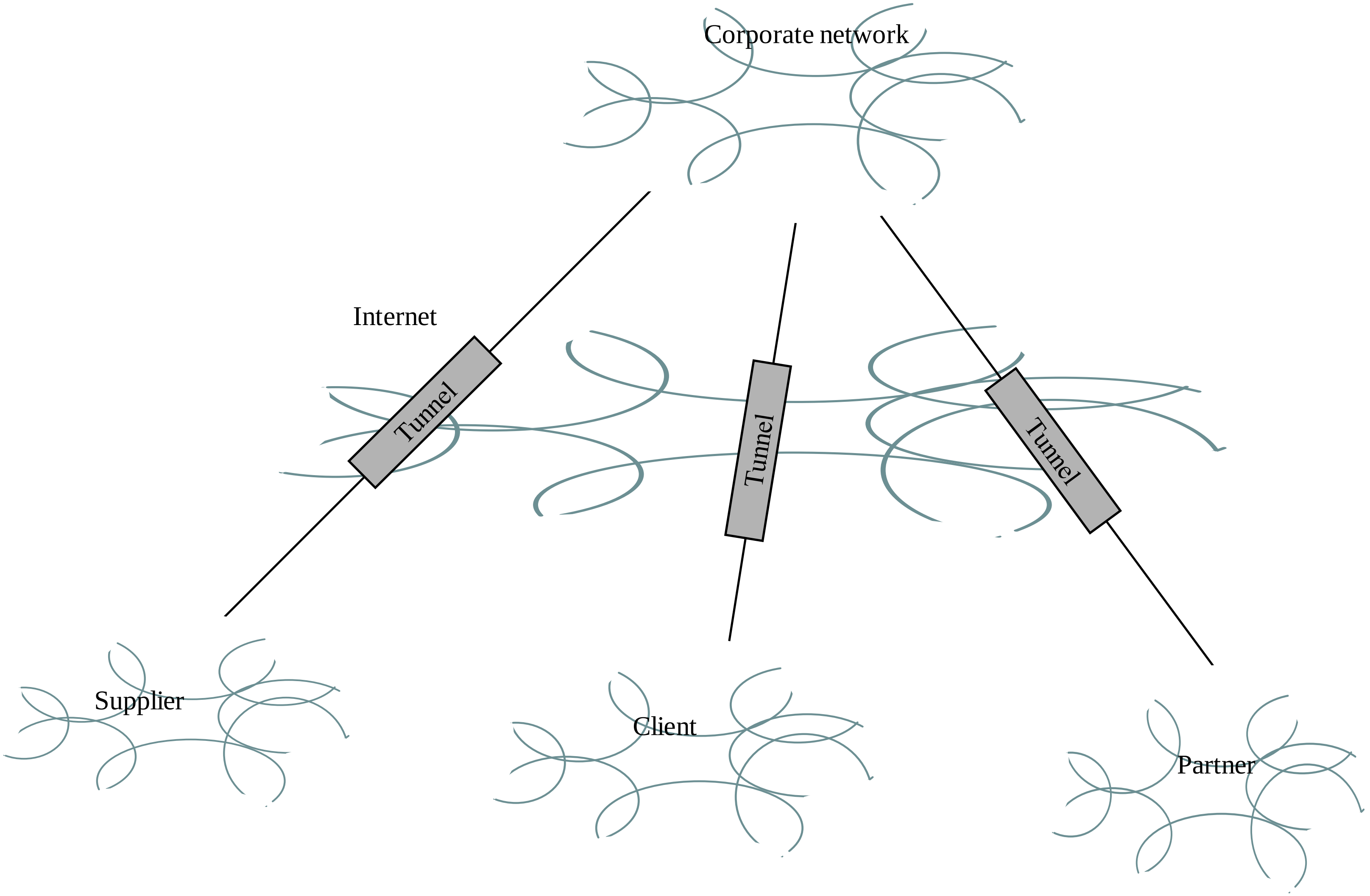
Intranet VPNs

- Advantages
  - Using a VPN over an ISP is much cheaper and more bandwidth efficient than setting up corporate network using leased lines
    - Maybe no need for dedicated WAN links
- Disadvantages
  - Can be slow
    - No guarantees of bandwidth through ISP unless Service Level Agreement obtained

Extranet VPNs

- Allow controlled access by partners, clients and customers to some of our sensitive information
  - our stock on hand
  - our availability to work on a project
  - contract work
- Needs to be very tightly controlled
- Many more variations than remote access and intranet
  - Less well defined term
  - Could include
    - password controlled access to website
    - SSH access to server

Extranet VPNs



General VPN requirements

- Security
  - Firewalls and NAT, User and Packet authentication, Encryption
- Availability and reliability
  - Service Level Agreements from ISPs
    - Do you need the ISP to have redundant routing, access and infrastructure?
- QoS
  - Best effort, Relative, Absolute
- Compatibility
  - IP gateways for non-IP traffic such as FR, IP tunneling
- Manageability
  - Need to be able to manage remote and local sites

VPN architectures

- Building blocks
  - VPN hardware
  - VPN software
  - organisation’s security infrastructure
  - service provider’s security infrastructure
  - public networks
  - tunnels

VPN hardware

- VPN servers
  - Dedicated servers running VPN server software
  - Functions are:
    - Listening for VPN requests
    - Negotiating connection requirements
    - Authenticating and authorising VPN clients
    - Accepting and forwarding data from clients
    - End point of VPN tunnel
      - VPN client is the other end-point
  - VPN servers often integrated into the firewall

VPN hardware

- VPN clients
  - Remote or local machines that initiate a VPN connection to a VPN server and login to the remote network
  - Usually software based but can be hardware based
- VPN routers
  - Similar to ordinary routers in that they find and select paths to remote networks
  - But may have additional features such as IPSec or path redundancy
- VPN concentrators
  - Aggregate multiple VPNs into the one device
- IP gateways
  - translate non IP traffic to IP traffic

VPN hardware

- Virtual Private Routers
  - Implemented at the ISP
  - Logical partitioning of a physical router at the ISP
  - Each partition provides full private router functionality to individual users
- Virtual Private Trunking
  - Implemented within the ISP
  - Provide switching functions for non-IP protocols such as Frame Relay
  - Based on Permanent Virtual Circuits and Switched Virtual Circuits

VPN Software

- VPN server software
  - The popular server software systems support VPN server functionality
    - Windows server, Linux, FreeBSD
- VPN client software
  - Most of the popular client software systems support VPN client functionality
    - Windows XP onwards
    - May require loading of compatible software
- VPN management software
  - Usually integrated with the VPN server software

Organisation’s security infrastructure

- Firewalls
  - Control access to trusted network
- Authentication systems
  - Allows appropriate access to authenticated users
- IPSec
  - Provides data encryption and authentication between
    - Client to server
    - Client to router
    - Firewall to router
    - Router to router

Service provider’s security Infrastructure

- Reliability and availability through redundancy
- Security through appropriate hardware and software
  - firewalls, authentication, encryption
- Supports main tunneling protocols
- Supports a variety of access networks

Public networks

- What technologies do we expect to run the VPN over?
- Commonly used public network technologies
  - ADSL, Frame Relay, Cable Modem
- Important to understand the difference between the Internet and the public networks
  - The Internet is an **overlay** network
  - It is built to use other network technologies

VPN architectures

- Many different ways of characterising VPN architectures
- Implementer based
  - who (ISP or subscriber) implements the VPN?
    - Dependent VPNs
    - Independent VPNs
    - Hybrid VPNs
- Security based
  - where in the network are the VPN endpoints?
    - Router to router
    - Firewall to firewall
    - Client initiated

VPN architectures

- Layer based
  - Link layer (layer 2)
    - PPTP, L2TP
  - Network layer (layer 3)
    - IPSec
  - Transport layer (layer 4)
    - SSTP
- Class based
  - Purpose, size and complexity of VPN
  - Class 0 to Class 4

Implementer based

- Dependent VPNs
  - service provider (ISP) provides complete VPN system
  - service provider implements the tunnels to and from the subscriber's sites
  - service provider implements NAS, RADIUS
  - Suitable for small organisations
- Independent or in-house VPN
  - Entire responsibility is the subscriber organisation's
  - subscriber implements tunnels between sites across Internet
  - Has own NAS, RADIUS etc
  - Most common implementation
    - secure, not that much more expensive than Dependent VPN for moderate to large organisations

Implementer based

- Hybrid VPN
  - Combination of dependent and independent approaches
  - Part of the VPN is provided by the ISP and the other by the subscriber
  - Typical implementation is for tunneling to be provided by the ISP and Authentication by the subscriber
  - Another typical implementation is for the use of multiple ISPs
    - provides redundancy should one ISP fail

Security based

- Router to router VPNs
  - VPN tunnel is constructed between the routers as needed
- Firewall to Firewall VPNs
  - Similar to Router to router VPNs
  - Usually implemented with IPSec
- Client initiated VPNs
  - Client to firewall/router VPNs
  - Client to server VPNs
- Directed VPNs
  - layer 5 (session layer) VPN
  - Data encrypted at layer 5
  - SOCKS v5

Layer based

- Link layer VPNs
  - PPTP, L2TP, SSTP
- Network layer
  - IPSec
- Transport layer
  - SSTP over SSL/TLS

Class based

- Class 0: small organisations, VPN server and client, PPTP, firewall
- Class 1: small to medium size organisations, DES Encryption, key exchange, authentication, one VPN gateway
- Class 2: medium size organisations, IPSec, 3DES, IKE, multiple VPN gateways, some high speed access options
- Class 3: ISP connectivity with SLA, directory services, IPSec and 3DES, IKE, multifactor authentication, 10 or more VPN gateways, RADIUS, NAT, high speed access
- Class 4: as for 3 but with greater capacity and additional high speed access options

Conclusion

- Looked at types of VPNs, VPN building blocks and ways of classifying VPNs
- Types of VPNs
  - remote access, intranet and extranet
- Building blocks of a VPN
  - VPN hardware and software
  - organisation's and service provider's security infrastructure
  - public networks
  - tunnels
- Many ways of classifying VPNs
  - who implements it
  - where the endpoints are
  - its size, services and complexity