SIT706
Cloud Computing Technologies

Week 10 Class-1

Networking – Deep Dive

Week 10-Class 1: Outline

- Networking – Deep Dive
  - Basic Concepts
  - Traffic Management
  - Virtual Networking
  - Networking Clouds
  - Virtual Private Clouds

Basic Concepts

Basic Concepts

1. Computer networks
2. Main Network Devices
3. Specialist Devices
4. Home/SOHO (Small Office Home Office) Networks
5. Enterprise Network Devices

Basic Concepts: Computer networks

- Computer networks represent the means through which we **interconnect computers** for the purpose of **data interchange**
- Applications are then **built on top** of this data interchange,
  e.g., email, web, storage, and so on.

Basic Concepts: Computer networks

- Networks can be broken into:
  - **Devices** for accessing the network,
    e.g., interface cards (NICs) in PCs/laptops/servers, tablets, phones, etc.
  - **Interconnection technologies**,
    e.g., Ethernet cabling (CAT 5/5e/6/etc.),
    fiber optic (OM1, OM2, OM3 and OM4), DSL (digital subscriber line) over telephone wire, WiFi, etc.
  - **Network devices** (as follows)

Basic Concepts: Computer networks

- Optical Fibre Cable Type OM1, OM2, OM3 and OM4:
- Multimode fibers are identified by the OM ("optical mode") designation as outlined in the ISO/IEC 11801 standard
- OM1, for fiber with 200/500 MHz*km overfilled launch (OFL) bandwidth at 850/1300nm (typically 62.5/125um fiber)
- OM2, for fiber with 500/500 MHz*km OFL bandwidth at 850/1300nm (typically 50/125um fiber)

Source: http://www.cablek.com/technical-reference/fiber-optic-cable-types

Basic Concepts: Computer networks

- Optical Fibre Cable Type OM1, OM2, OM3 and OM4:
- OM3, for laser-optimized 50um fiber having 2000 MHz*km effective modal bandwidth (EMB, also known as laser bandwidth), designed for 10 Gb/s transmission.
- OM4, for laser-optimized 50um fiber having 4700 MHz*km EMB bandwidth designed for 10 Gb/s, 40 Gb/s, and 100 Gb/s transmission.

Source: http://www.cablek.com/technical-reference/fiber-optic-cable-types

Basic Concepts: Computer networks

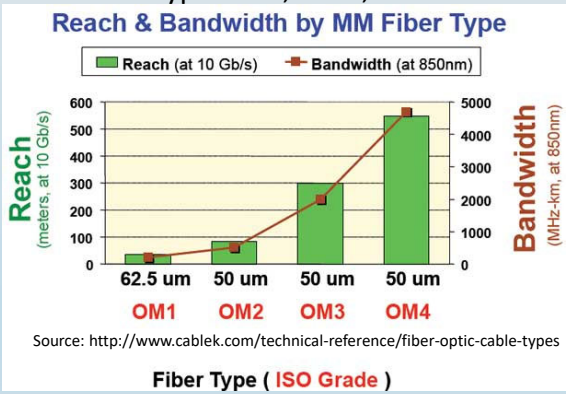
- Optical Fibre Cable Type OM1, OM2, OM3 and OM4:

A stripped multi-mode fiber

Source: https://en.wikipedia.org/wiki/Multi-mode_optical_fiber

Basic Concepts: Computer networks

- Optical Fibre Cable Type OM1, OM2, OM3 and OM4:



Source: http://www.cablek.com/technical-reference/fiber-optic-cable-types

Basic Concepts: Computer networks

- Optical Fibre Cable Type OM1, OM2, OM3 and OM4:

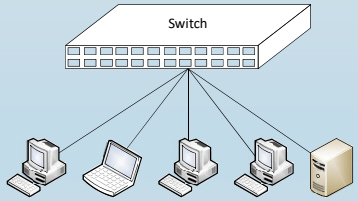
Fibre Type (ISO Grade)

Fiber Types and Reach			
Fiber Type	Bandwidth* Length Product (MHz*km or GHz*m)	10GBASE-SR Distance (meters)	40GBASE-SR4 and 100GBASE-SR10 Distance (meters)
OM1	160-200	33	N/A
OM2	400-500	82	N/A
OM3	2000	300	100
OM4	4700	400	150

Source: http://www.cablek.com/technical-reference/fiber-optic-cable-types

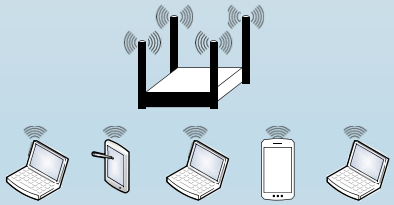
Basic Concepts: Main Network Devices

- **Switches**: used to connect multiple network devices via cable forming a Local Area Network
  - Most commonly IEEE802.3 Ethernet networks running at speeds of 100Mbps, 1Gbps, and 10Gbps, with 40Gbps starting to appear and 100Gbps in standards development



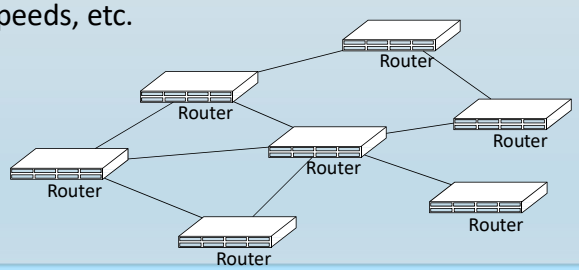
Basic Concepts: Main Network Devices

- **WiFi Access Points**: used to connect multiple devices via wireless transmissions forming a LAN
  - Most commonly IEEE802.11 networks running at speeds of 54Mbps(802.11a/g), up to 600Mbps(802.11n), or up to 6.93Gbps(802.11ac)



Basic Concepts: Main Network Devices

- **Routers**: used to connect multiple networks together forming a Wide Area Network. Routers can be wired or wireless devices.
  - Many transmission mediums, technologies, speeds, etc.



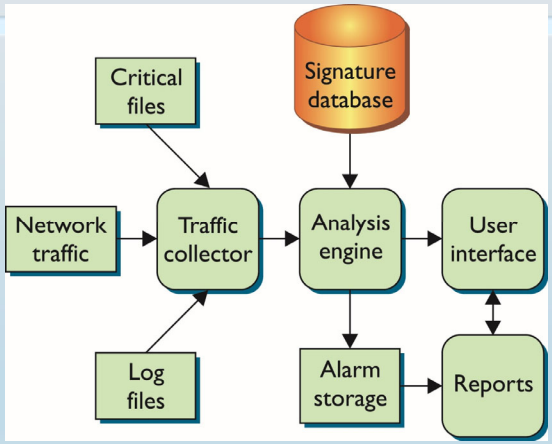
Basic Concepts: Main Network Devices

Router

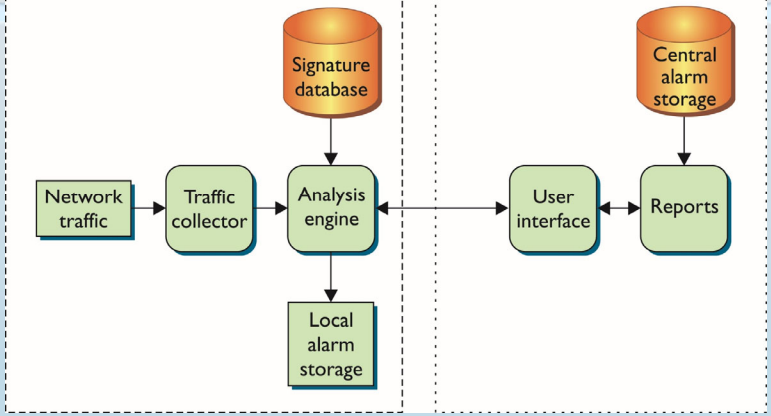
Basic Concepts: Specialist Devices

- **Firewalls**:
  filter network traffic on protocol information or even the content of data sent over the network
- **Intrusion detection/prevention systems**:
  detect and potentially take action to thwart/prevent network attacks by recognising patterns in network traffic

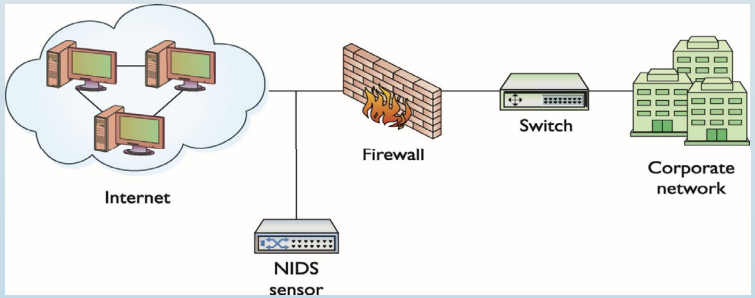
IDS Components



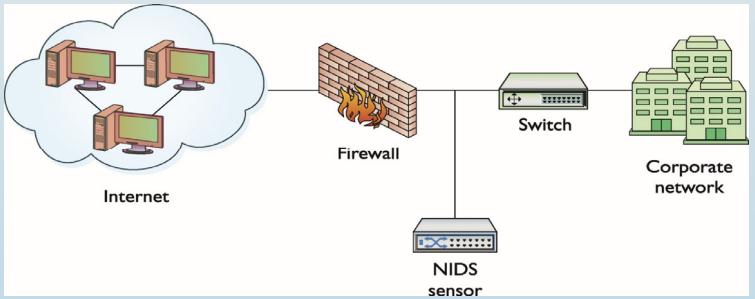
Network IDS Components



Network IDS



Network IDS



Basic Concepts: Specialist Devices

- **Load balancers**:
  redirect traffic to one of several servers to distribute load across multiple devices (forming a cluster)
- **Transparent web browsing caches**
  - ✓ Devices supporting **VoIP**, video conferencing, etc.
  - ✓ And so on.

Basic Concepts: Home/SOHO Networks

- Share the same technologies as above but usually **combine devices and cheap hardware**
  e.g., most ADSL routers include an ADSL modem, basic router functionality, basic switch functionality, and a WiFi Access Point.
  NBN is another option and NBN speed is faster than ADSL2+
- Most of the work is often **performed in software**
- **Seldom work at full capacity**,
  e.g., a file is downloading very slowly but now web browsing is also very slow

Basic Concepts: Enterprise Network Devices

- An **enterprise network** decreases communication protocols, facilitating system and **device** interoperability, as well as enhanced internal and external **enterprise** data management.
- Usually perform a **limited number of functions**, e.g., only a switch, only a router
- Most of the work is **performed in hardware** supported by specialist operating systems
- Have more **powerful processing capabilities**
- May support traffic loads that **exceed capacity**

Basic Concepts: Enterprise Network Devices

- Often support functionality that has **no relevance in home networks**, e.g.,
  - **Failover functionality**: if the main router fails another can automatically take its place
  - **Quality of Service**: ability to tag and process traffic differently,
    e.g., prioritise VoIP traffic, restrict/cap bandwidth usage for file transfer, etc.

Traffic Management

Traffic Management

- Network traffic management deals with the process of monitoring and controlling the activities of network besides transforming the network into a managed resource by improving performance, efficiency, and security.
- It also helps to operate, administer, and maintain the network systems.

Traffic Management

- Network traffic Types:

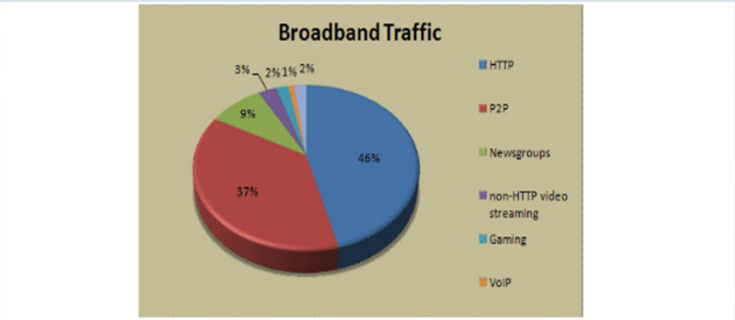
Traffic Type	Example	Problem	Solution
Bursty Traffic	Downloads of FTP, graphic, video content	Consumes high bandwidth and Starves applications	Set constraint to limit access to bandwidth
Interactive Traffic	SSL transactions, IM, Telnet sessions	Susceptible to competition for bandwidth and results in poor response time	Prioritize over less essential traffic
Latency Sensitive Traffic	Streaming applications, Voice over IP, video conferencing	Susceptible to competition for bandwidth and results in poor response time	Set minimum and maximum bandwidth range based on priority
Non-Real Time Traffic	Email, batch processing applications	Consumes bandwidth during business hours	Schedule bandwidth during non-business hours

Source: https://www.ipv6.com/applications/network-traffic-management/

Traffic Management

- **Internet Traffic Management:** Also known as application **traffic management**, refers to tools that monitor the flow of Web application **traffic** over a network.
- These tools route **traffic** among multiple devices within a network, limiting delays and freeing bandwidth.
- Today's Internet traffic is very different from that of early days' internet.
- As it is growing exponentially with ever-increasing web pages, full length movies, software applications, and online games, the need for an effective network traffic management is on the stage. Some of the facts and figures are:

Traffic Management



Data source: Ellacoya Networks

Traffic Management

1. Home Networks
2. Enterprise Networks
3. Increase Traffic Control
4. Virtual LANs

Traffic Management: Home Networks

- **Home networks** are usually very **simple** as they usually have:
  - **Several devices**
  - **One Internet connection**
  - **One network**

Traffic Management: Enterprise Networks

- **Enterprise networks** are usually divided into several "subnetworks" (subnets)
  - **Subnets for public use**
  - **Subnets for private use** usually divided by role, e.g.,
    - Student and Staff access networks
    - VoIP networks
    - Video conferencing networks

Traffic Management: Enterprise Networks

- **Enterprise networks** are usually divided into several "subnetworks" (subnets)
- **Advantages of using subnetting**: It is useful to control and to reduce the network traffic by limiting number of broadcasts.
- It is allowed any organization to **subnet** its network without needed to have a new network IP through an internet service provider (ISP).

Traffic Management: Enterprise Networks

- According to networkcomputing.com there are five advantages of using subnet:
  - ✓ **Improve network performance and speed**
  - ✓ **Reduce network congestion**
  - ✓ **Boost network security**
  - ✓ **Control network growth**
  - ✓ **Ease administration**

Traffic Management: Enterprise Networks

- **Enterprise networks** are usually divided into several subnets such as:
  - **Subnets for public use**
  - **Subnets for private use** usually divided by role, e.g.,
    - Student and Staff access networks
    - VoIP networks
    - Video conferencing networks

Traffic Management: Increase Traffic Control

- **Use multiple subnets** to increase control of traffic, e.g.,
  - Some subnets can have **high priority** (VoIP, video conferencing)
  - Some subnets can have **additional protection** (staff/student access)
- This can be **based on simple network techniques**, however, this **requires additional hardware** which quickly becomes **expensive**

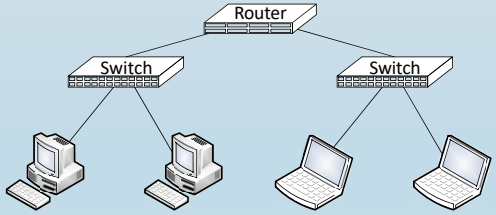
Traffic Management: Virtual LANs

- Apply the concept of Virtual LANs (VLANs) to **reduce the (above) additional hardware and expense**
- Virtual LANs (VLANs) allow network administrators to subdivide a physical network into separate logical broadcast domains.
- **VLAN** is a **logical grouping of networking devices**. **When we create VLAN, we actually break large broadcast domain in smaller broadcast domains. Consider VLAN as a subnet**
- A switch can be used for multiple networks

Traffic Management: Virtual LANs

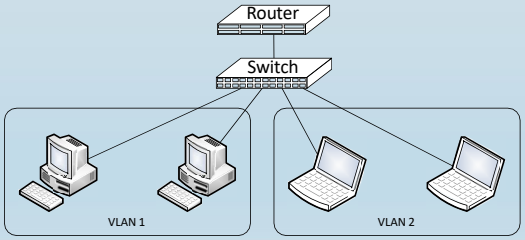
Example:

- Consider the following 2 networks interconnected by 1 router
- Can those **2 switches be replaced by 1 switch**?



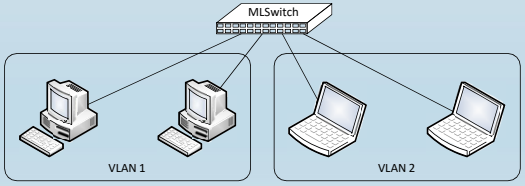
Traffic Management: Virtual LANs

- A **switch can manage VLANs** for multiple networks
- For example, **simple VLANs allow 2 networks to be interconnected by 1 switch**



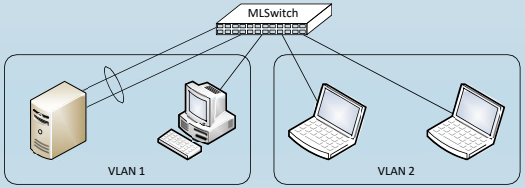
Traffic Management: Virtual LANs

- A **multilayer switch** is a switch that also includes router functionality.
- The (previous) **router and switch** can be replaced by a **multilayer switch**.



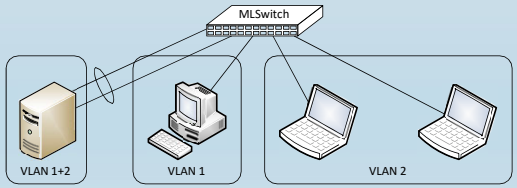
Traffic Management: Virtual LANs

- **Link aggregation** is combining network connections to provide:
  - **more bandwidth capacity** than one connection
  - **redundancy**



Traffic Management: Virtual LANs

- Connections can also be configured to carry **more than one VLAN**

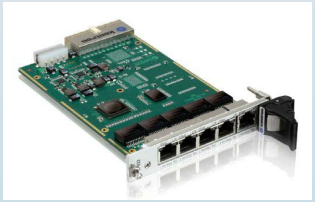


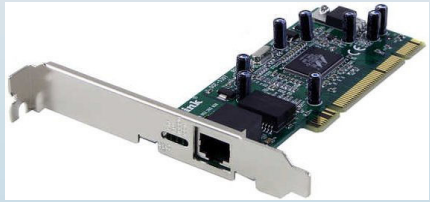
Virtual Networking

Virtual Networking

1. Network Interface Cards (NICs) and Switches
2. Virtual Network Interface Cards
3. Virtual Switches
4. Additional Abstraction Layer

Network Interface Cards (NICs) and Switches





Virtual Networking: Virtual Network Interface Cards

- Virtual network interface cards are virtual network interfaces that are based on the physical network interface cards of a host.
- Each host can have multiple network interface cards, and each network interface card can be a base for multiple virtual network interface cards.
- A virtual NIC (vNIC) **mimics** a physical NIC (pNIC)
- When configuring a virtual machine (VM), the **virtual hardware can include 0 or more vNICs**
- **vNICs are connected to vSwitches**

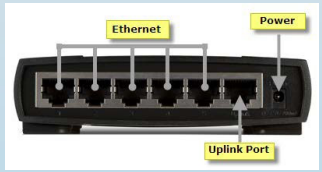
Virtual Networking: Virtual Switches

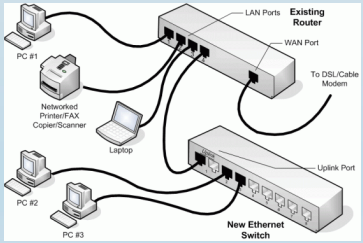
- A vSwitch **mimics** a pSwitch
- There are some **minor differences** such as how MAC[1] addresses are learned
  - pSwitches **learn by monitoring traffic**
  - vSwitches **already know** MAC addresses of connected VMs
- **A virtual switch is a software program that allows one virtual machine** (VM)**to communicate with another**.

1. A Media Access Control (MAC) address is a unique identifier assigned to a network interface.

Virtual Networking: Virtual Switches

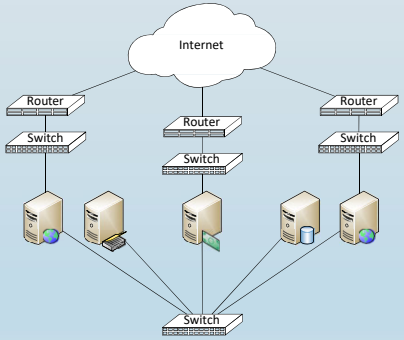
- pSwitches are **limited** by the number of ports (how many cables can be plugged in)
- vSwitches are **not limited**
- pSwitches include an "uplink port"





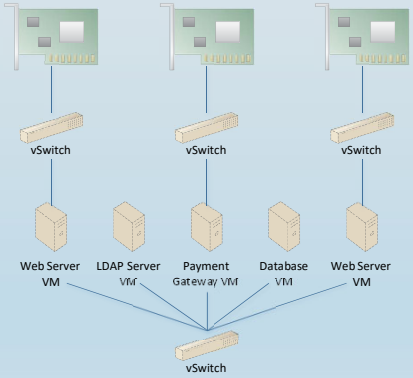
Virtual Networking: Example

- Consider the following physical topology



Virtual Networking: Example

- The same topology can be represented using virtual networking:



Virtual Networking: Additional Abstraction Layer

- Using vNICs and vSwitches provides an additional **abstraction layer**
  1. Allows pNICs to be **shared** by multiple VMs
  2. Allows vSwitches to be **distributed** across multiple physical hosts
     (the **virtual network topology on the previous slide could be on one or more physical hosts**)

Virtual Networking: Additional Abstraction Layer

3. Allows traffic to be **captured**
   (for VM snapshots, live backups, etc.)
4. Allows traffic to be **redirected**
   (for VM/storage migration)
5. Allows traffic for one cloud consumer to be effectively **isolated** from other cloud consumers
6. Allows traffic generated by a VM to be carefully **filtered** before reaching the physical networks

Networking Clouds

Networking Clouds

1. Existing Technologies
2. Other Technologies
3. VLANs
4. Private VLANs
5. Software Defined Networking (SDN)
6. Why is SDN useful?

Networking Clouds: Existing Technologies

- Networking infrastructure for building clouds is merely an **extension of existing technologies**
  - **Construction of clusters** in the data centre are supported by **very high speed networks**
  - Introduction of **link aggregation** for high throughput
  - Introduction of LAN and WAN redundancy for high availability, such as **multihoming**
  - Introduction of **software defined networking** (SDN) to provide the ability to **program a network**

Networking Clouds: Other Technologies

- Very large physical hosts can have **many high speed NICs**
- **Problem**: Each time data is received or successfully sent, the NIC will send an interrupt to the CPU for the operating system (hypervisor)
  - **Each interrupt** causes some **overhead**, reducing performance slightly
  - **Many interrupts** can make this performance reduction **significant**

Networking Clouds: Other Technologies

Three solutions:

1. VLANs
2. Private VLANs
3. Software Defined Networking

Networking Clouds: VLANs

- each NIC can receive **one or more** VLANs
- **minimising** this number:
  - **reduces** unnecessary traffic
  - **improves** performance

Networking Clouds: Private VLANs

- **isolates network traffic** using three port types:
  1. **Promiscuous ports**: communicate with **all** other ports in the VLAN
  2. **Isolated ports**: only communicate with **promiscuous** ports
  3. **Community ports**: only communicate with **promiscuous** ports and other ports in the **same community**

Networking Clouds: Software Defined Networking (SDN)

- Software-defined networking is not a technology, but an architecture that provides support for virtual machine mobility independent of the physical network.
- In the traditional approach to networking, most network functionality is implemented in a dedicated appliance; i.e., switch, router, application delivery controller.
- In addition, within the dedicated appliance, most of the functionality is implemented in dedicated hardware such as an ASIC (Application Specific Integrated Circuit).
- The traditional data network has been largely hardware-centric.

Networking Clouds: Software Defined Networking (SDN)

- Functionality in a network device, e.g., a switch, can be roughly divided into:
  - **Data plane**: functionality for **forwarding data** through the device
  - **Control plane**: computes **how data is forwarded**, providing that information to the data plane (e.g., route calculations)
  - **Management plane**: functionality for network administrators to **monitor and configure**

Networking Clouds: Software Defined Networking (SDN)

- SDN aims to:
  - **move the control plane** out of the physical device and **into software** such as the VIM

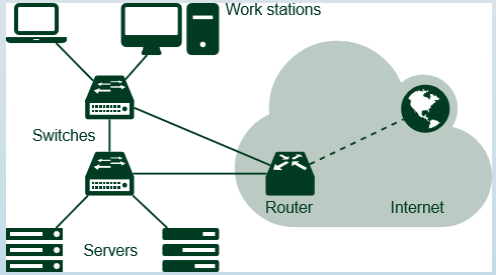
Networking Clouds: Why is SDN useful?

- Historically networks were **static**
  - Network administrators **manually configure** new devices
  - Networks **rarely change**, once operational
  - As a result, network configuration management was a **very carefully planned and controlled** process

Networking Clouds: Why is SDN useful?

- Consider cloud computing:
  - New VMs **easily deployed** with a few mouse clicks
  - VMs **migration**, manually or automatically
  - As VM migrate, **communication paths move**
  - **Isolate traffic** of one cloud consumer from others
- The **network is constantly changing**, it is no longer static.

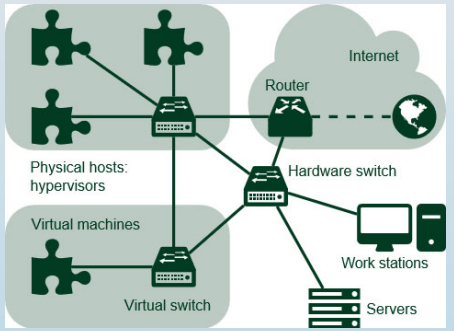
Networking Clouds: SDN



A traditional wired LAN, with hardware switches

Source: Quentin Monnet

Networking Clouds: SDN

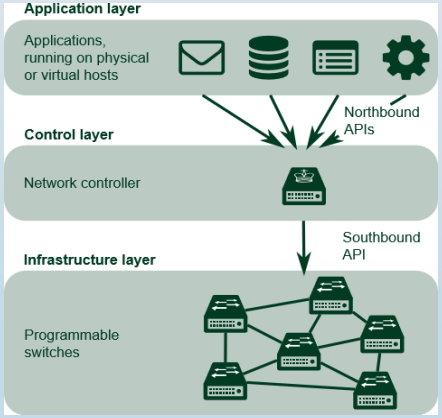


Network with "VM to NIC" and "VM to VM" traffic

Source: Quentin Monnet

Networking Clouds: SDN

SDN architecture concept



Source: Quentin Monnet

Virtual Private Clouds

Virtual Private Clouds

1. Virtual Private Clouds
2. Virtual Private Network (VPN)
3. VPN Technologies

Virtual Private Clouds

- Virtual Private Clouds effectively allow **resources from different clouds to be combined together**
  - Allows **the cloud to become an extension** for existing datacentre equipment, e.g., cloud bursting, hybrid cloud
  - Allows **cloud services**, deployed by different cloud consumers, to **interconnect** in a custom network topology
  - Allows **cloud services**, deployed on different cloud providers, to **communicate securely**

Virtual Private Clouds

- Note: **Amazon Web Services** includes a generalised Virtual Private Cloud service
  - ✓ Cloud consumers can define one or more virtual network architectures on which to run their applications
  - ✓ The additional services provided by AWS are beyond the scope of this class

Virtual Private Clouds: Virtual Private Network (VPN)

- A key technology for establishing Virtual Private Clouds is VPNs
  - ✓ VPNs, or Virtual Private Networks, allow for private data to be securely exchanged over a public network
  - ✓ Uses cryptography to protect data passing over public networks

Virtual Private Clouds: Virtual Private Network (VPN)

- Two types of VPN:
  - ✓ Remote Access VPN: temporary connection, usually used for remote/mobile users to securely connect to the services of their workplace
  - ✓ Site-to-Site VPN: permanent connection between two locations on the Internet ensuring all data passing between those locations is secured, e.g., from private cloud/infrastructure to public cloud

Virtual Private Clouds: VPN Technologies

- There are a several VPN technologies, including:
  - ✓ Point-to-Point Tunnelling Protocol (PPTP): Encryption: RC4
    - Released by Microsoft with Windows 95 and commonly available but has several security issues potentially allowing data to be exposed (don't use)
  - ✓ Secure Socket Tunnelling Protocol (SSTP): Encryption: SSL
    - Replacement of PPTP by Microsoft with release of Windows Vista but not as widespread as other technologies (avoid)

Virtual Private Clouds: VPN Technologies

- There are a several VPN technologies, including:
  - ✓ Layer 2 Tunnelling Protocol (L2TP)/IPsec:
    Encryption: DES, 3DES, or AES
    Internet standards combining tunnelling (L2TP) with secured IP communication (IPsec), but may be blocked by firewalls
  - ✓ OpenSSL:
    Encryption: 3DES, AES, RC5, or Blowfish
    Open source VPN using SSL/TLS (same as https) and generally more reliable and faster than the above alternatives, but has limited support on mobile devices

Virtual Private Clouds: VPN Technologies

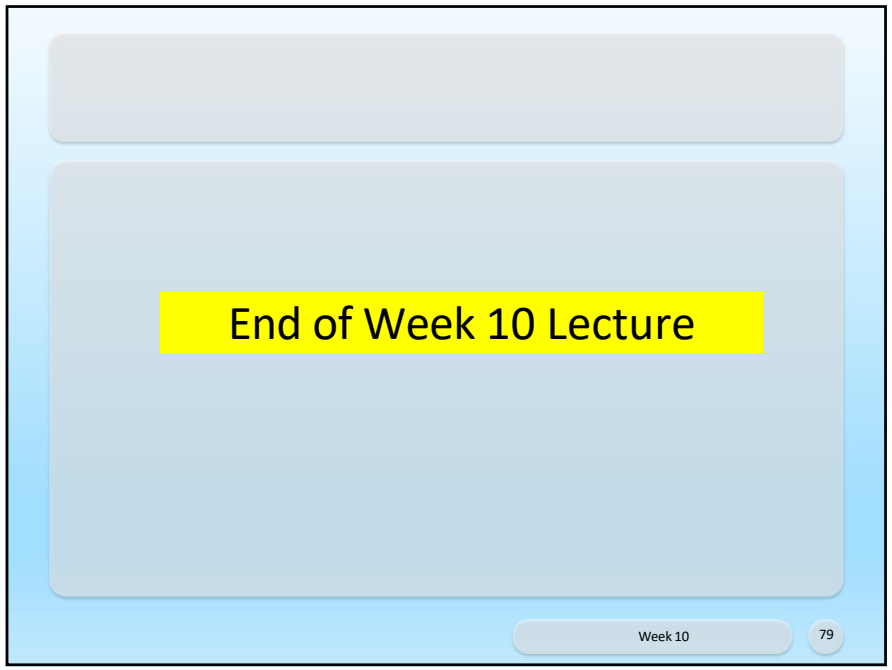
- There are a several VPN technologies, including:
  - ✓ VPN Connect / Internet Key Exchange version 2 (IKEv2):
    Encryption: 3DES or AES
    Relatively new technology developed by Cisco and Microsoft which can automatically re-establish a VPN connection (good for mobile), but not as widely available

Week 10-Class-1 Summary

- Networking – Deep Dive
  - Basic Concepts
  - Traffic Management
  - Virtual Networking
  - Networking Clouds
  - Virtual Private Clouds

Next Week(Week 11)

- Review the lectures: week-1 to week10
- Exam Hints.


End of Week 10 Lecture
Week 10
79