



Prifysgol Cymru

Y Drindod Dewi Sant

University of Wales

Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

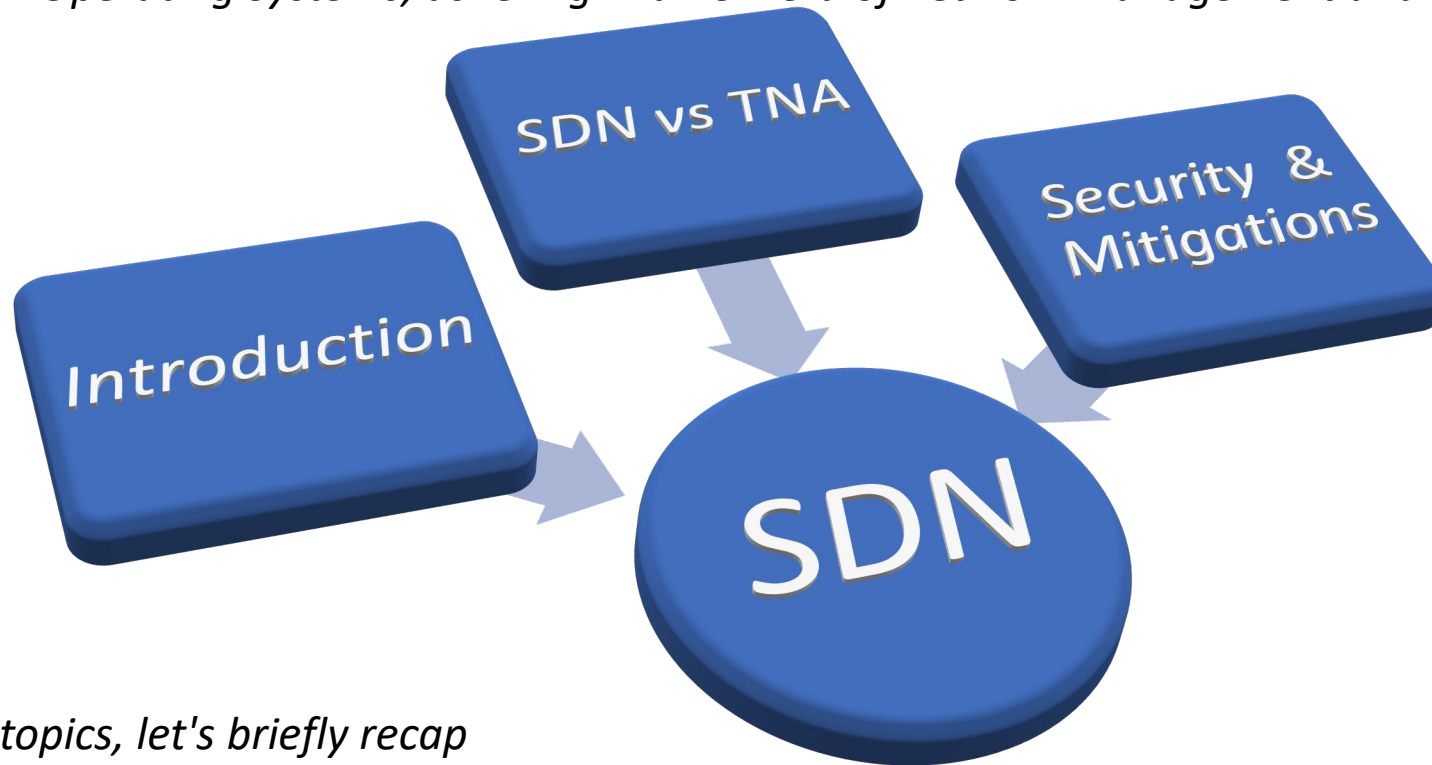
SDN

Network Operating Systems and Services ACCA5023

Today's Discussion

Today's discussion will delve into the realm of Software Defined Networking (SDN). In our Network Operating Systems module, we've explored a plethora of services offered by Network Operating Systems, particularly focusing Windows Server 2022 environment. From IP Addressing to Active Directories, DNS, DHCP, VPN, and beyond, we've laid a solid foundation.

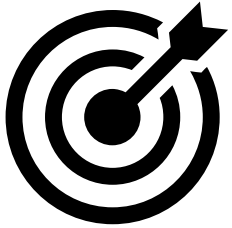
Now, we're taking the next step by delving into the world of PowerShell scripting and execution. Furthermore, we'll explore how SDN integrates with Network Operating Systems, ushering in a new era of network management and optimization.



Before we dive into today's topics, let's briefly recap what we covered so far.



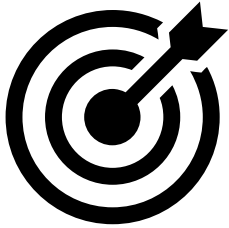
Milestone



Coursework 1:

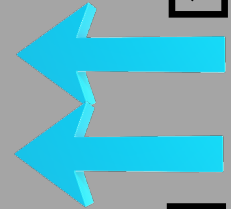
- ✍ Choose your Hypervisor based on your research (Q.2.1)
- ✍ Download (use Evaluation Copy) and Setup your Virtual Machines – as per the topology (Q. 2.2)
- ✍ Research on IP Address (Based on the Group Discussion earlier)
- ✍ Download Debian Linux
- ✍ Configure IP Address for Windows Server and Client – Successful Ping
- ✍ Install Debian Server and Client
- ✍ Configure IP Address for Debian Server and Client – Successful Ping
- ✍ Test and Troubleshoot (if required) your network.
- ✍ Research on Routing and Network Services.
- ✍ Submit your Coursework 1 – **03/03/2026**





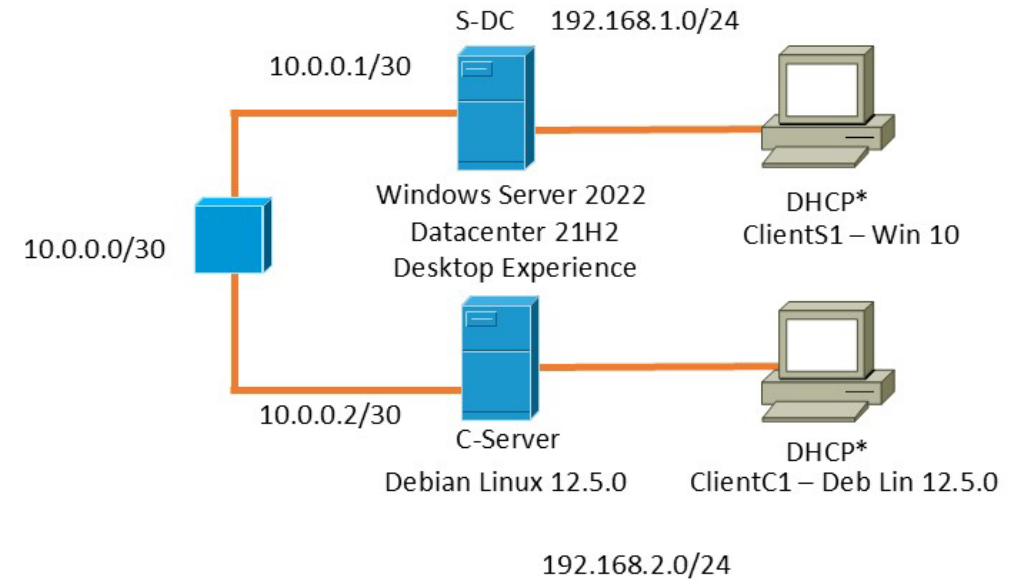
Coursework 2:

- ✍ Coursework 2 – Walkthrough
- ✍ Plan to work on your Topology – Gantt Chart !!! (Reading Week)
- ✍ Continue with your Topology – Firewall Rules/ Policies
- ✍ Installing RRAS Services, AD-DC, DNS, S2S VPN
- ✍ Configuring DHCP, Mount Second Disk, Export/ Create User Accounts
- ✍ Work on other Aspects (Sharing Disk Drive, IIS Server, RDS)
- ✍ Troubleshoot if necessary
- ✍ Submit your Coursework 2 – **11/05/2026** (Submission: 1500)



50 M

1. Routing: **10 M**
 - a) **Modify Firewalls**
 - b) **Install Routing and Remote Access**
 - c) **Persistent IP Forwarding**
2. Domain Server (Swansea) **10 M**
 - a) **Promote Domain Controller**
 - b) **DNS A Records, Reverse Lookups**
3. Domain Membership **5 M**
 - a) **Domain Membership CS1, LCD, CL1**
4. Encrypted Connection between Swansea and London **5 M**
 - a) **VPN – Persistent Connection**
5. Users **5 M**
 - a) **PowerShell Scripts/ Manual Addition**
6. DHCP Server **10 M**
 - a) **DHCP Server and Relay**
7. Test and Troubleshoot **5 M**
 - a) **All Machines Ping Successfully**

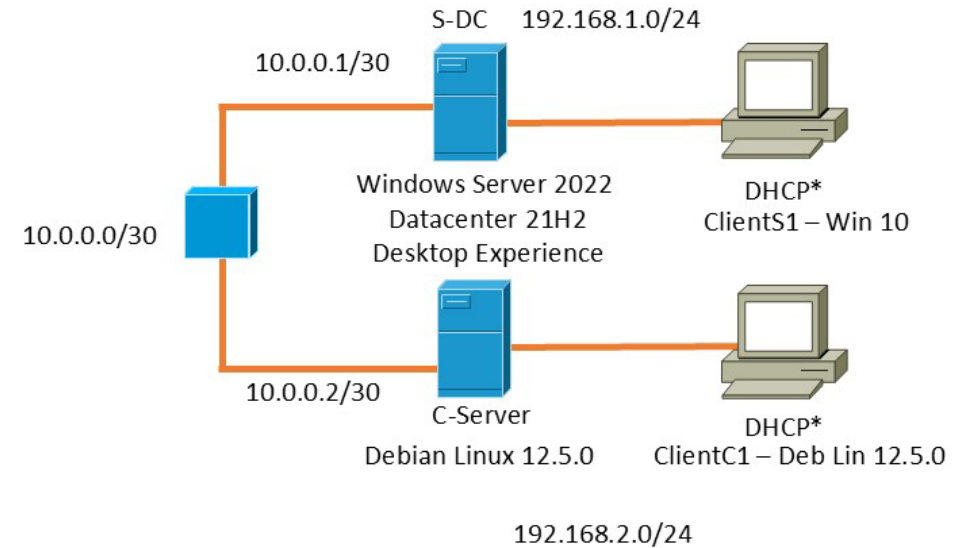


* Will do when DHCP Services are installed

3 Weeks Before Easter Break

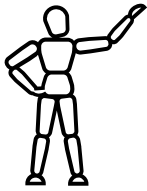
35 M

1. Disk Drive: **15 M**
 - a) Mount E:\ SwanseaFiles **5 M**
 - b) Sharing Disk Drive in both Swansea and London **5 M**
 - c) Full Control Permission **5 M**
2. IIS Server **10 M**
 - a) Create a Website with Internal Authentication **5 M**
 - b) All Users Authenticated **2 M**
 - c) Presented with “Welcome Message” **3 M**
3. Remote Desktop Services **10 M**
 - a) Successful remote desktop access **5 M**
 - b) Create a Login page (HTTP/HTTPS) **1 M**
 - c) Functional [HTTPS://rds.yourname.acca](https://rds.yourname.acca) **2 M**
 - d) Fully Functional [HTTPS://rds.yourname.acca](https://rds.yourname.acca) with Certificates **2 M**



* Will do when DHCP Services are installed

Action



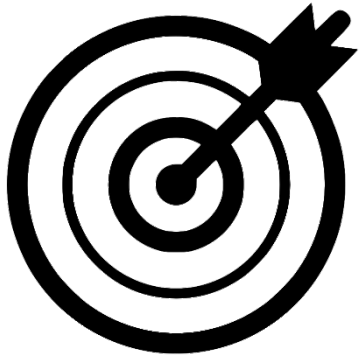
As we conclude today's lecture with PowerShell Scripts. This will help you in ensuring efficient network configuration, management and troubleshooting. I would strongly recommend you start using PowerShell Scripts in your Coursework to gain more or comprehensive understanding.

I trust you equip yourselves with the knowledge and skills necessary to effectively implement the concepts required in your coursework, fostering a deeper comprehension of their configuration and operation within network environments.

By actively working in writing scripts and executing them, you will solidify your understanding of theoretical concepts and cultivate practical skills essential for implementing your network effectively in real-world scenarios. With this foundational knowledge in place, I encourage you to

✍ Continue to work on your coursework and complete all the tasks as per the plan above

Objectives



[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

- ✍ Understand PowerShell Scripts
- ✍ Continue with your Coursework 2
- ✍ Submit your report – **11th May 2026 @ 1500**
- ✍ Demonstration – **12th May 2026**

PowerShell: Introduction

What is PowerShell Scripting?

- Automation of tasks.
- Storing frequently performed steps in files.
- Writing statements in PowerShell language.
- Storing statements in a text file (.ps1).
- Aimed at automating repetitive tasks.

Benefits of PowerShell Scripting

- Time-saving: Execute scripts to save time.
- Reusability: Easily reuse existing solutions.
- Efficiency: Focus on more valuable tasks.
- Handle various system modifications and side effects.
- Allows for easy reuse of scripts.

one command = one task

multiple commands in a script = full automation

PowerShell: Introduction

Features of PowerShell Scripting Language

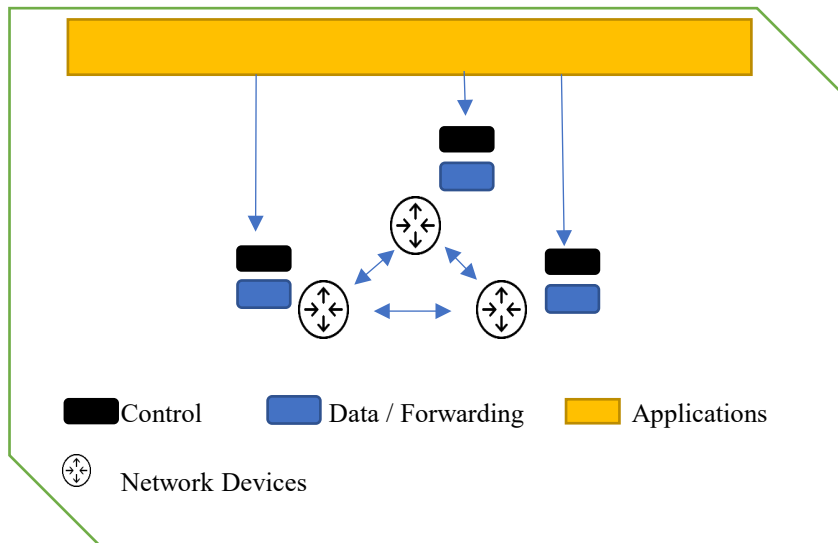
- Variables
 - Store values for reuse.
 - Can be used as arguments for commands.
- Functions
 - Named lists of statements.
 - Produce output in the console.
 - Can be used as input for other commands.
- Flow Control
 - Control execution paths with constructs like If, Elseif, Else.
- Loops
 - Operate on arrays, inspect each item, perform operations.
 - Includes conditional looping with Do-While loops.

PowerShell: Introduction

Features of PowerShell Scripting Language

- Error Handling
 - Write robust scripts to handle errors.
 - Differentiate between terminating and nonterminating errors.
 - Use constructs like Try and Catch for error handling.
- Expressions
 - Used frequently in scripts for custom columns, sorting, etc.
 - Represent values in PowerShell syntax.
- .NET and .NET Core Integration
 - PowerShell provides integration with .NET and .NET Core.
 - Enables powerful functionalities beyond the scope of this module.

Introduction



Legacy Network Architecture

The existing network infrastructure (addressed as Legacy Networks)

- the IP based protocols are based on the TCP/IP standards which are widely used in network communications.
 - better utilization of all the resources available and focus on all the specification of data starting from data formats, its transmission, addressing, routing till the data being received at the destination.
 - Enabling the existing standards to allow high throughput in the networks.
-
- Automatic reconfiguration and other response mechanisms have no concentration in the existing standards.
 - The communications between networks are heavier which raises the risk of increasing “performance” bottlenecks.
 - In the case of larger network size and during the increase of delay or bandwidth in a network, the potentiality of IP Networking is a big Question.

*The focus now laid on the physical routing devices.
network map & forwarding data packets is in one function.*

Introduction

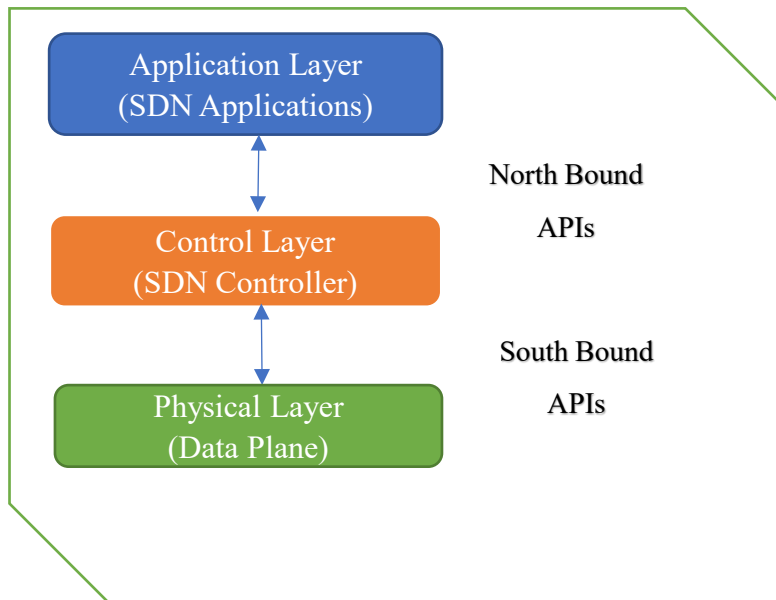
Software Defined Networking

- an upside-down epitome considering the existing network operations.
- a decoupled architecture with centralized control
- very cost effective and complexity impact technology.
- implicate closed networks & vendor specific proprietary implementations.
- Intelligence and flexibility provided to the control plane by decoupling it from data plane.
- This fundamental change in the operation brings linear perspective towards the approach of resolving the existing problems of the IP Networking Architecture.

SDN Architecture

SDN is a technology which helps in virtualization of physical network devices based on “On Demand” requirements.

Introduction

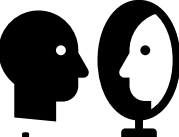


SDN Operational Structure

Software Defined Networking

- The SDN architecture is a layered approach classified with three layers.
- The topmost layer is the application layer, where the applications dedicated or designed for the entire network control and operations are residing on various servers.
- The bottom most layer is the Physical Layer or a Data Plane layer which acts as a forwarding engine.
- The arbitrate layer in between the Application Layer and the Physical Layer is the Controller or a Control Plane layer rendering network services for the physical layer.
- The Application and the Control Layer relates to the North Bound Interface.
- The Control Layer and the Physical Layer relates to the South Bound Interface.

A logical centralized view over the network not only achieving flexibility but also cost efficiency and feasibility



Introduction

Application Layer

Network Management, Security,
Automation, Bandwidth, Policy, Topology.

Control Layer

Routing Controls, Network Discovery,
Mapping, Southbound Plugins.

Data Layer

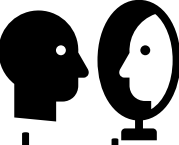
Physical Switches, Virtual Switches.

SDN Functional Attributes

Software Defined Networking

- The SDN approach minimizes the overload and throughput in a network caused by the physical devices by separating the control and the data plane.
- The operations of control and data plane in the SDN does not rely of a physical networking device but a flow based forwarding decisions.
- This flow based forwarding decisions will enable a better flexible data transmission which would be based on the topological requirements.
- This is an evident of ensuring a logical centralized view over the network not only achieving flexibility but also cost efficiency and feasibility.
- The control plane (Layer), which is a software platform, is not in the physical networking devices as in a legacy network, instead providing logically centralized view on the network and poses control.

The SDN implemented networks hold control over the flow of data in the network



Introduction

Software Defined Networking

- There are various controllers and protocols playing key roles in making the layers work effectively and efficiently.
- SDN Controllers: NOX, POX, FloodLight, FlowVisor, Beacon, Maestro, SNAC, RISE, OpenDaylight, IBM, HP etc.
- The North Bound API, connecting the control plane and the application layer aims to desegregate the applications which are developed for customizing the network with the SDN Controller.
- The South Bound API establishes the communication between the data and the control plane (controller and the physical) to commute configurations, flow entries etc.

All the information to the data paths such as switches/routers are given through southbound application programming interface.

History

1997 AT&T

- GeoPlex a common IP Software Platform developed by AT&T acted as a managing network middleware.

2001 Ericson

- First soft switch known as Supranet Transaction Server.

Today's SDN concept was formulated in 2007 and then taken forward by Stanford University in 2008.

The arising need of programmable network and implications in legacy network, Open Networking Foundation (ONF) came into existence in 2011.

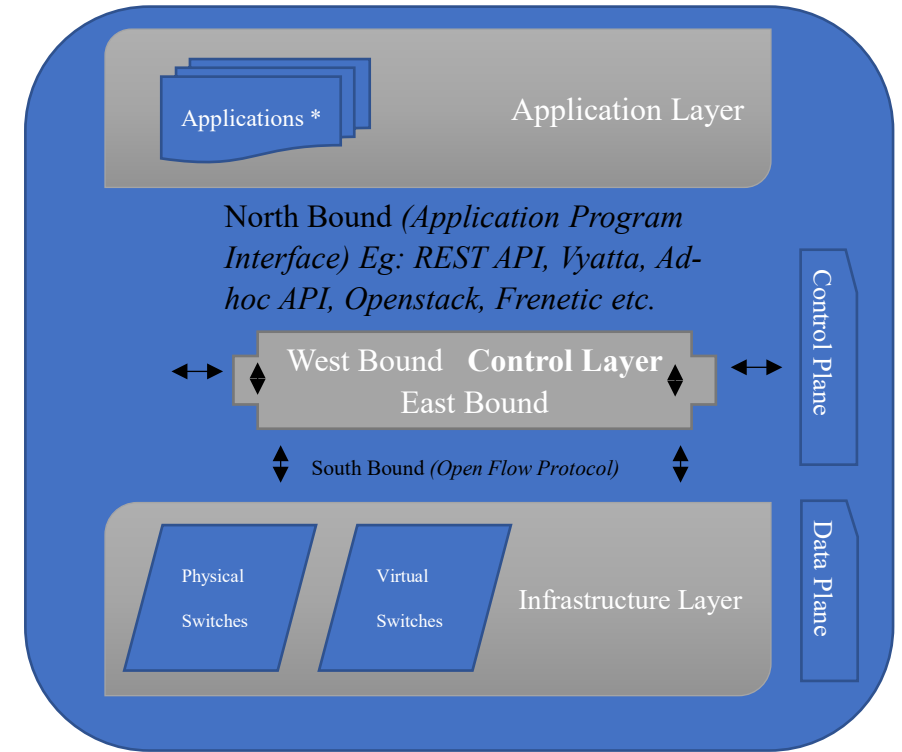
If doing a SWOT analysis over SDN, the cost is reduced and its overall control features increase exponentially providing an eagle's view control.

SDN has many advantages over a traditional network likely to solve many security issues of a legacy network.

Nevertheless, SDN also has many security vulnerabilities.

Need

- **Exponential increase in the number of users** in a network exposing high risk of security in a network.
- There are a huge **number of security breaches and counter – attacks in enhancing the security aspects**, are continuously happening in the networking domain.
- However, **the attackers are still a step upfront in compromising a network**.
- SDN Architecture would provide a fine-grained opportunity **to detect and mitigate Attacks in the network because of its decoupled design**.
- The **programmable design** in SDN will enable a feasible solution in detecting the attacks very quickly and act accordingly by **making required changes in the Packet Forwarding**.

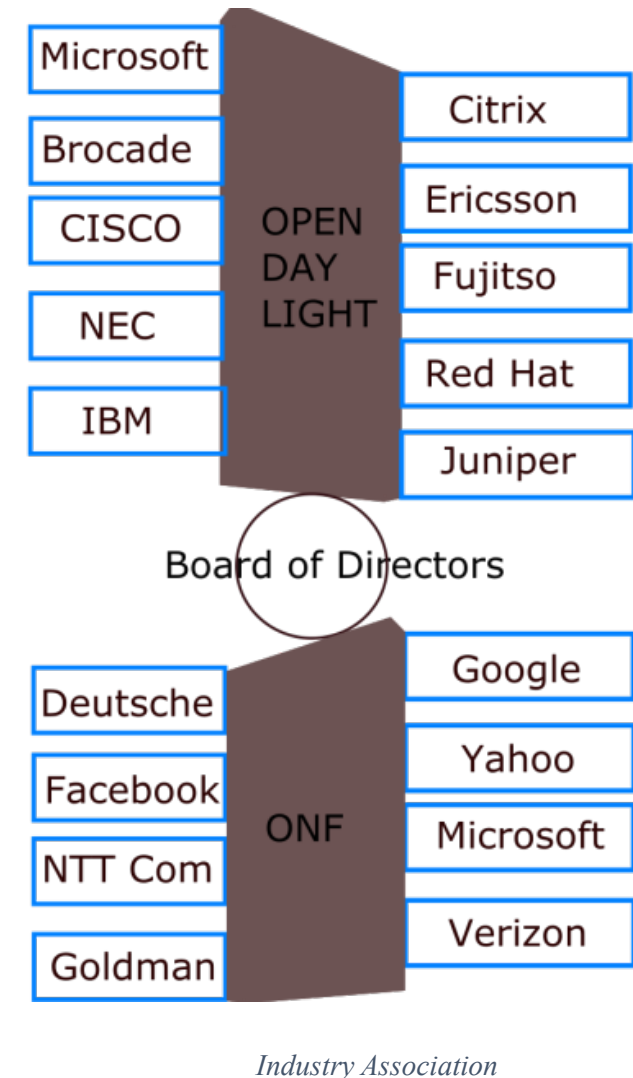


SDN Architecture

- As detailed earlier, the heart of SDN Architecture is its Control Plane where the **controller sits with an eagle view** making a variable control over the network.
- All the networking devices fall under data plane, easing itself just by forwarding the traffic. However, traffic forwarding is adapted from the instructions of the controller in the Control plane.
- Hence, the packet is sent from the data plane as a **“PacketIn” message** into the **Control plane** as instructed by the controller and those instructions are **defined by the applications** in the Application layer.

SDN Standards

- There are two perspectives of standards in SDN.
 - IETF (Internet Engineering Task Force) standard is a true standard body &
 - the other standards ONF (Open Networking Foundation), OpenDayLight, OpenStack are all industry alliance standards.
- This figure self explains the participation of Industry in the development of SDN Technology.
- These industrial giants join in different perspectives and portfolios to form a non-profitable organization to establish standards in the SDN technology.
- This made the technology to cross over 42 billion US dollars in the year 2022 which is projected as a growth rate of over 72.3% (ARC, Forecast(2020 - 2025)).
- Internet Engineering Task Force is one standard which is not related to any of the industrial participation, anticipating true standard specifications.
- The other standards like ONF, ODL, etc which are collaborative with industry alliances



SDN - Industry

- Google, Amazon, Verizon and many more enterprise organisations have already started to switch over their operations towards Software Defined Networking.
- Google started to work on SDN in 2008 and initial deployment was done in 2010.
- In the recent past, dynamic flow control is implemented in the Varmour firewall product for an enterprise network.
- Recent deployments were done by
 - Cornell University,
 - REANZZ – New Zealand,
 - ToulX – France,
 - Géant – Switzerland.

SDN - Efforts

- SDN Architecture would be accessed based on the following performance criteria

- **Performance**

- *A network infrastructure's capability is primarily based on the processing speed. The speed on the network is calculated by the throughput and latency as metrics. On considering the above parameters, SDN has an improvised performance scope comparing with traditional networks because of its programmability.*
- *However, limitations such as 10 GBPS links in physical layers needs further research works to mitigate problems like high volume of data flows.*

- **Scalability**

- *From the initial stage of its development, SDN architecture's ability to make itself flexible for the growth of the network maintains the research scope on a rising mode.*
- *Even though, it is decoupled in the control and data functionalities, and all of it done with a centralised controller, which is considered as a hero in this overall architecture, it could cause high impact on network scalability.*

SDN - Efforts

- SDN Architecture would be accessed based on the following performance criteria

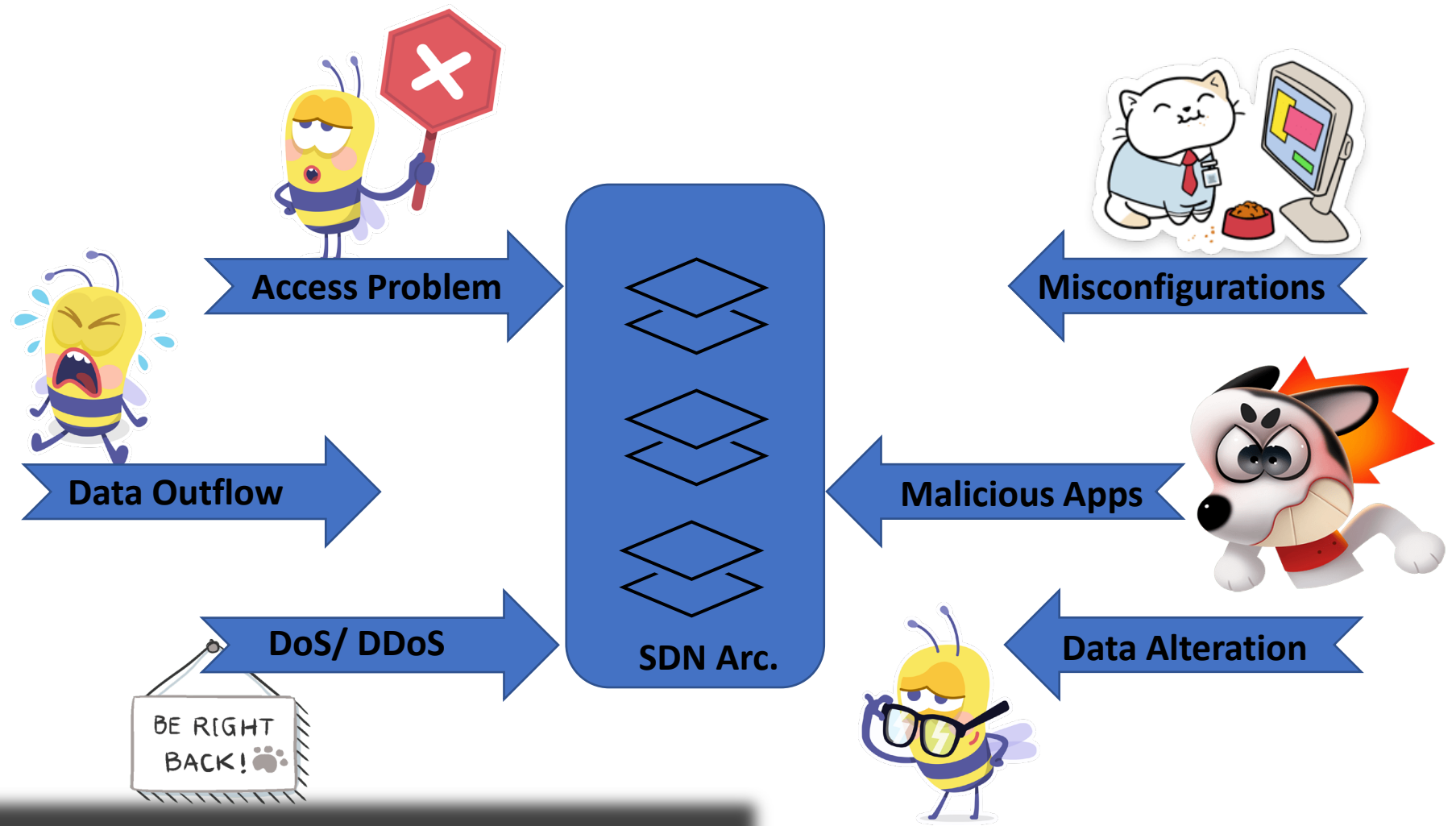
- **Availability**

- *Availability is another critical criterion for a network's rating. The network's functioning capability and its balance on responding to the requests. Functionally, SDN's availability is extensively better compared with the traditional networks because of its decoupled approach.*
- *However, the heart of the SDN network operation is its controller and if the controller is made unavailable, the entire networks availability is a big question mark.*

- **Security**

- *In an approach to bring forth a network architecture to mitigate the problems existed in, more than a couple of decades existing traditional network architecture, SDN made its way because of its totally new approach of decoupling scenario, promoting vendor independent modules within a network.*
- *As, all the basic functional parameters for a network has evidenced augmented pros and cons in an SDN Architecture comparing to a traditional network, additional but essential in today's cyber world, "security" also remain in the same position necessitating to address more distinguished challenges.*

SDN Security



Software Defined Networking has the potential to secure its network

SDN Security

Untrusted control over
Application, Control and Data Plane,
as they are decoupled.

Attack focusing Data Plane
modules/ entities
(Switches/ Virtual Networks)

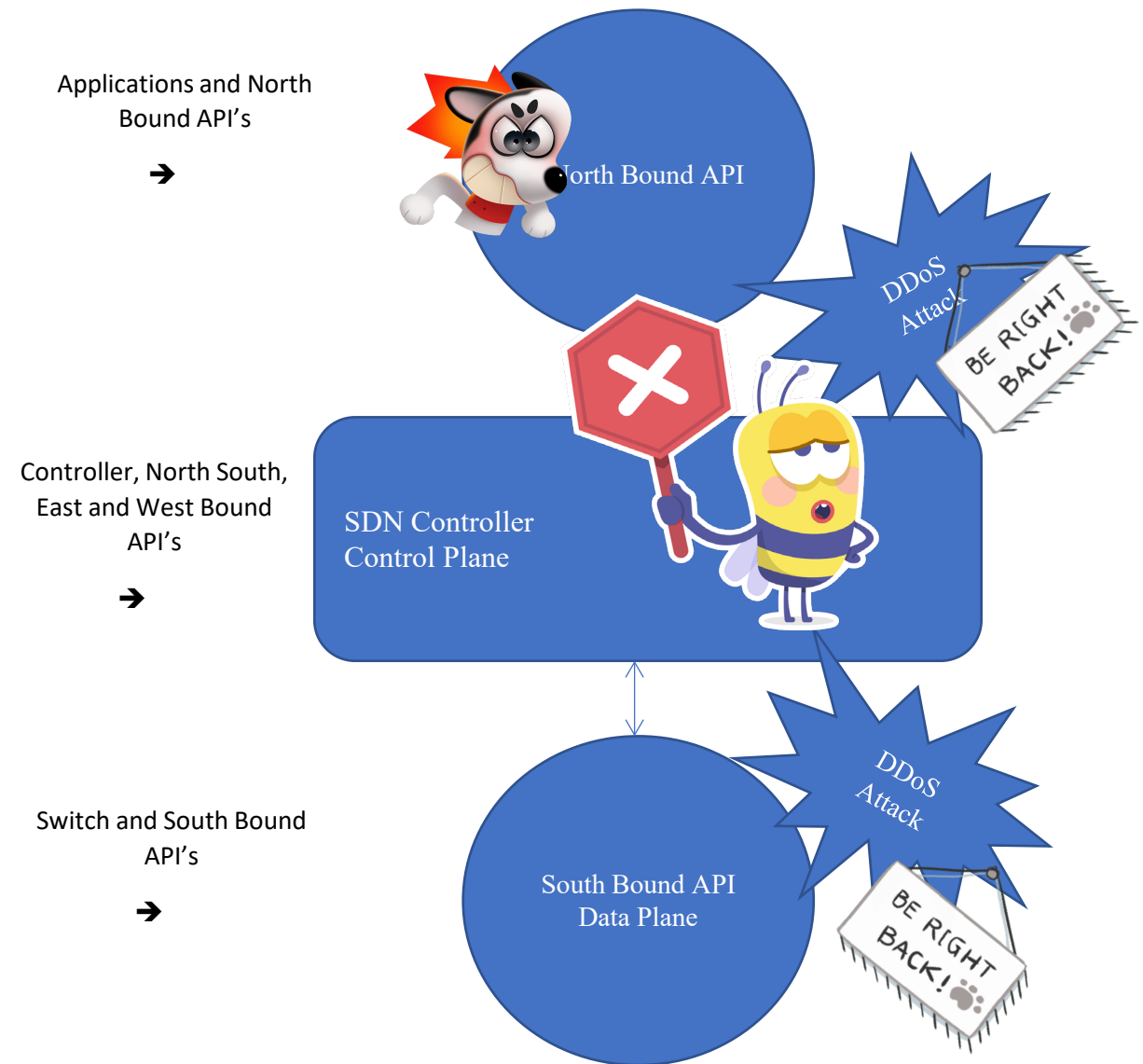
Attack focusing Control Plane
(Controllers and its deliverables)
Altered traffic in the network

- This makes a sense that, a **controller** in SDN Architecture is the **boss** supported by the **decision support system** entities in the **application layer** and the instructions are followed by the task-doers, actual devices in data plane.
- The importance of **Application Layer** is now clear, that it could modify the flow of data plane using external applications.
- **Application Layer** is also one of the **vital resources** in an SDN Architecture, as it focuses on **operations and functions** of the network such as *Routing, access control, security, load balancing* etc.

On a security aspect, Software Defined Networking has an upper hand in detecting and reacting to DDoS attacks

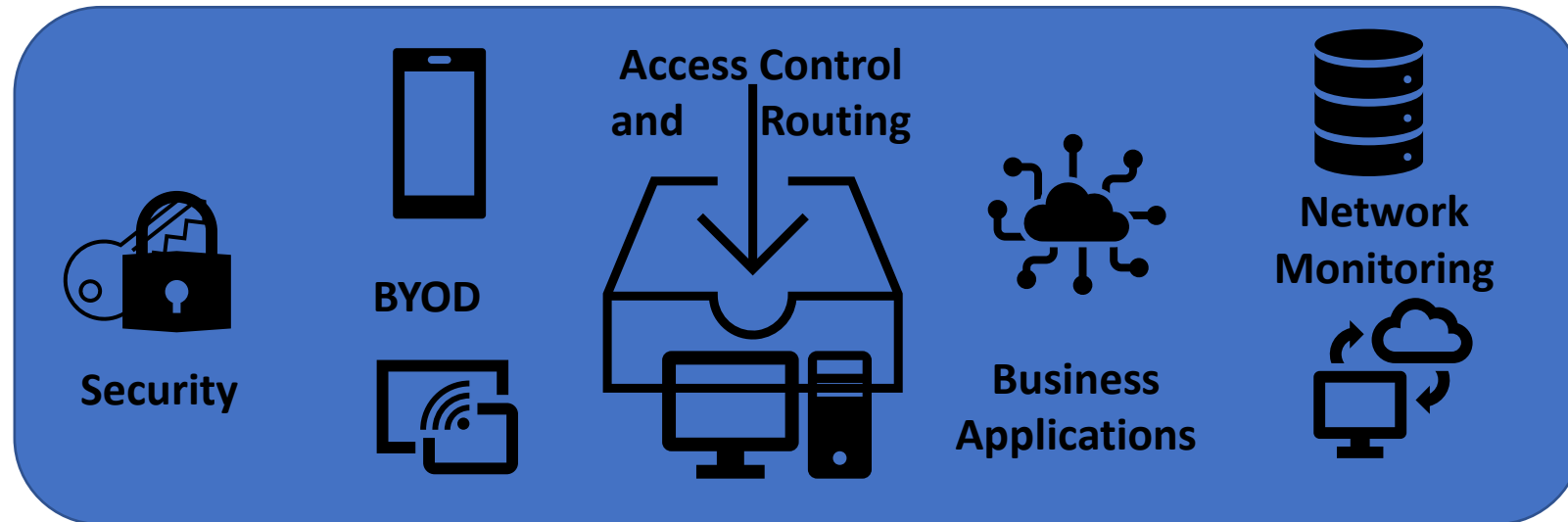
SDN Security

SDN is used to provide security in the network by improving the security itself



SDN Application Layer Vulnerability

The **Application layer** of Software Defined Networking architecture often deals with end-user applications that are utilized for security purposes, load balancing, network virtualization etc.



SDN Application Layer Vulnerability

- The major focus on application layer is its level of *trust management* between the applications and the SDN architecture.
- The major weak point at the application layer is the *trust over the communication between the application and the controller* leading to various attacks like *spoofing, malicious applications, flow control modifications* paving an easy way to diverse models of attacks including *DDoS attacks*.
- DDoS attacks are primitive due to its attack nature of being easy to plunge and not easy to defend.
- Using *botnets via a malicious application to control/ block the point of communication* between the application layer and the controller or other legitimate applications could lead to a devastating network collapse.

SDN Security Mitigation Techniques

- Let us move with the CIA Triad in mitigating the security issues, as it is a proven method.
- The parameters of CIA Triad
 - **Confidentiality:** The network architecture should be restricting the access and disclosure of any information only to authorized users to avoid misuse
 - **Integrity:** The network architecture should be viable to ensure and confirm the trustworthiness of information to avoid unauthorized alteration
 - **Availability :** The network architecture should be available and ready to provide the expected service to the authorized users.
- To ensure a secured network,
 - the data flow within the network must be confidential
 - the entire system must be bound with integrity and
 - the availability of the network must be ensured by making redundant infrastructure.

SDN Security Mitigation Techniques

According to ONF, 8 security principles has been outlined which are applicable to all the SDN protocols, SDN components and SDN interfaces.

- Principle 1: Clearly Define Security Dependencies and Trust Boundaries
- Principle 2: Assure Robust Identity
- Principle 3: Build Security based on Open Standards
- Principle 4: Protect the Information Security Triad
- Principle 5: Protect Operational Reference Data
- Principle 6: Make Systems Secure by Default
- Principle 7: Provide Accountability and Traceability
- Principle 8: Properties of Manageable Security Controls

Diolch/Thank You Any Questions?

Books Referred: *Dauti, Bekim. Windows Server 2019 Administration Fundamentals: A beginner's guide to managing and administering Windows Server environments, 2nd Edition . Packt Publishing.*

Links referred in this presentation:

- Microsoft Virtual Academy