1.Prepare for implementation of network routers and switches

1.1 Prepare for given job according to work health and safety (WHS) and environmental requirements with appropriate personnel

1.2 Identify safety hazards and implement risk control measures in consultation with appropriate personnel

1.3 Determine nature and scope of network routers, network switches and network resources from job briefs or appropriate personnel

1.4 Select and obtain network services and network application requirements according to enterprise procedures

1.5 Obtain identified operating instructions, manuals, hardware and software testing methodologies

1.6 Consult appropriate personnel to ensure the task is coordinated effectively with others involved at the worksite

Legislation, workplace health and safety (WHS), codes, regulations and standards

Ready, set, go!

1
Prepare for it

2
Do it

3
Conclude

So, before you start, consider

Is my services regulated under any law/licensing requirements? E.g. do I need a license?

What is the situation of the existing system? E.g. knowing your “patient” before undertaking a “surgery”.

Does the site have suitable environment for my devices? E.g powersuply, temperature and humidity.

Will I or my devices or my services cause any hazards to the workplace? E.g. noise, RF.

Do I have permission to access the system? E.g keys or RFID to the datacentre or passwords

In an IT context, your IT services might have been regulated by many rules.

What they are?

- Acts: legislate on a subject. Acts give a general overview of how to make workplaces safe and healthy.
- Code: Collection of acts
- Standards: specification of quality and norms. Regulations set out the standards you need to meet for specific hazards and risks, such as noise, machinery, and manual handling.
- Licences: a permission from an authority
- Organsiational Policies: requirements and guidelines conducting certain business

Summary of WHS/OH&S acts, regulations and codes of practice - Victoria

Victoria (Vic)

Act: *Occupational Health and Safety Act 2004* (Vic)

Regulation: *Occupational Health and Safety Regulations 2017* (Vic)

Codes: Vic Compliance Codes

Regulator: WorkSafe Victoria

Resources:

- Workplace Safety for Small Business
- Employer rights and responsibilities
- Make your workplace safer

Further reading

https://www.business.gov.au/risk-management/health-and-safety/whs-oh-and-s-acts-regulations-and-codes-of-practice

OHS issues –other regulations

Occupational Health and Safety Act 2004: This Act is the cornerstone of legislative and administrative measures to consistently improve occupational health and safety.

Occupational Health and Safety Regulations 2007:These regulations are made under the Occupational Health and Safety Act 2004.

AS 4801:Australian Standard 4801 outlines all requirements for implementing an occupational health and safety management system

Source: http://www.ohs.net.au/codes-of-practice and https://www.business.gov.au/info/run/workplace-health-and-safety

OHS issues –Code and Standards

Codes:

Model Code of Practice: Managing electrical risks in the workplace

Model Code of Practice: How to manage work health and safety risks

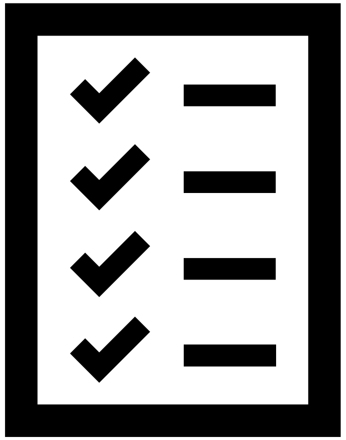
Sources: https://www.safeworkaustralia.gov.au/doc/model-code-practice-how-manage-work-health-and-safety-risks

Standards (AUSTRALIAN STANDARDS REFERENCED IN THE MODEL WHS LAWS (e.g.))

AS 4801:2001 Occupational health and safety management systems Regulation 5

AS/NZS 1269.1:2005 Occupational noise management—Measurement and assessment of noise emission and exposure Regulation 56

Source: https://www.safeworkaustralia.gov.au/system/files/documents/1705/information-sheet-australian-standards.pdf



Prepare for networking jobs according to legislation, WHS codes, regulations and standards

What legislation, work health and safety (WHS) regulations, codes and standards relevant to networking installation services?

How do you understand the importance of OHS induction and hazards disclosure?

Research and discuss

OHS procedures

Training and communications for WHS is essential for OHS procedures to be followed as expected.
People needs to Excises the Duty of Care. The organisation's OHS prosecutes provide guidelines on compliance with legal obligations, articulating roles and responsibilities of both the employer and employees.
They also outline safety standards
Identify the hazards and notification, emergency and evacuation
OHS procedures also define how to hand injuries and incidents, and more comprehensive tasks such as how to conduct a safety audit
The process to report and resolve WHS issues .

WHS factors you need to take into consideration

Building Management - Environmental impacts

Disclosing the following potential impacts and hazards:

- Electrical Safety: e.g. the use of Power-boards (EPOD), Extension leads, Testing and Tagging of these boards and leads, voltage requirements
- Noise from devices: disclose vendor's specification about noise level. LAeq,8h of 85 dB(A) for 8-4 shift workers, no exposure to above LC,peak of 140 dB(C). (https://www.safeworkaustralia.gov.au/noise)
- Radiation Safety: specification and proof of Radiation Safety: e.g. Maximum Exposure Levels to Radiofrequency Fields —3 kHz to 300 GHz
- Ergonomics: consider when adjusting your workstation.
- Laser Safety: Laser classification- Lasers are divided into seven classes according to accessible emission limits. Health effects of laser use (AS/NZS IEC 60825.14:201)
- Machinery and Equipment or Manual Handling: avoid hazardous manual handling, assess the risk you cannot avoid it, reduce the risk as far as possible, following instruction or licensing requirements when using Machinery and Equipment.

Use of Hazard Alerts and signs

Staff clearance and IDs so that the client can identify and recoginise you and provide supports.

WHS- for you and for your client

For you, what you need to know:

Is the place safe for me ?	Is the place suitable for my routers and other devices?	Am I working with other people?	What should I do if anything goes wrong?

For your client, what they need to know:

Are my services going to cause any WHS issues or hazards?	What supports does the client need to provide for me to install the routers and other devices?	Do they have any WHS policies	What should I do if anything goes wrong?

Technical requirements or safety issues?

Some technical requirements might be also a safety issue. Imagine routers, switches, servers are put in an office and the office is not air-conditioned properly. The devices might turn on fans to cool down, this actually generate more heat.

Routers and switches are very sensitive to humidity and overheating. At the same time, lack of ventilation leading to uncomfortable, hot and humid working conditions. And the issue might cause further risks to the devices and environment as well.

Also Humidity – low humidity can cause static electricity when there is static electric charges imbalanced within or on the surface of a material. While high humidity may also damage the devices. Given that air moisture content is a natural conductor, it even causes other serious safety issues.

A data centre (or a dedicated room) with proper environmental control would be necessary for both the proper functioning of the devices and the safety of the place.

See more on:

https://www.safeworkaustralia.gov.au/system/files/documents/1705/mcop-managing-electrical-risks_in_the_workplace-v3.pdf

Also See Australian Standard AS1668.2: *The use of ventilation and airconditioning in buildings - Ventilation design for indoor air contaminant control*.

Preparing the Site (Safety, Technical and Environmental Requirements for your network installation)

To address WHS regulations and compliance requirements, you need to follow the regulations as well as the following areas related to networking projects.
Specify the range, e.g. humidity for the devices to work properly.
Refer to the **vendor's user manual** or **installation guide.**

- Humidity Requirements.
- Temperature requirements
- Altitude Requirements
- Dust and Particulate Requirements
- Minimizing Electromagnetic and Radio Frequency Interference
- Shock and Vibration Requirements
- Grounding Requirements
- Planning for Power Requirements
- Rack and Cabinet Requirements
- Power supply

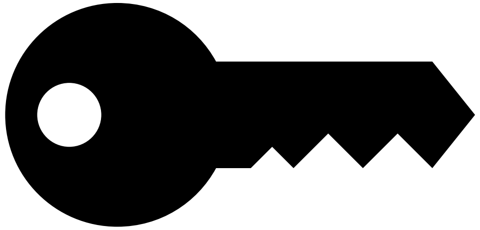
Obtain installation requirements and guidelines

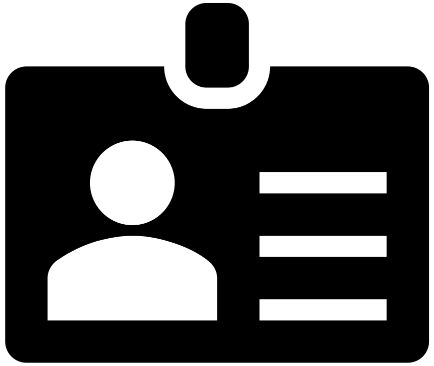
- Check the model and brand name of your devices.
- Find user manuals that came with the products.
- If there is no hardcopy, look up the vendor's website and find the data sheets or white paper for that particular model:

	Immunity: ● CISPR24: 2010 [+ amd 1 & 2] ◦ EN300386: V1.6.1 ◦ EN55024: 2010 ◦ EN61000-6-1: 2007 ◦ KN24: 2011 ◦ TCVN 7317:2003
Environmental operating range	● Nonoperating temperature: -40° to 158°F (-40° to 70°C) ● Nonoperating humidity: 5% to 95% relative humidity (noncondensing) ● Nonoperating altitude: 0 to 15,000 ft (0 to 4570 m) ● Operating temperature: 0° to 50°C (de-rate 1°C per 1000-ft increase in altitude) ● Operating humidity: 5% to 95% relative humidity (noncondensing) ● Operating altitude: 0 to 10,000 ft (0 to 3000 m)

Discussion

- What are some potential impacts and hazards networking installation and devices have?
- What are the technical requirements of your installation services?
- What are the environmental requirements of your installation services?





Preparation for site access

Summary of things you need to confirm/cordinate with your client before your installation

Access needs:

- Needs access to multiple sites where routers, switches, and other networking devices are located.
- Need to have data centre with environmental control and access control
- Need permission/access to system admin credential.
- May have access to confidential information.

Technical factors:

- Need to confirm power supply and environmental requirements
- Assess and obtain physical and logic access to the data centre or nodes
- Check existing security configuration and rectify existing issues.
- Have rollback plan for failure/data leak, consider encryption and backup.
- May be able to dump data being transmitted though routers and gateways.

Asking for site access

Specify the following:

- Who is coming and how to identify them, e.g. name badges, uniforms, smartcard/tag
- What they will bring in and out (system design)
- How long will they be staying (system design or action plan)
- What will be doing (system design or action plan)
- What supports will need: keys, offices, power supply, Wifi access, parking etc.
- Do they need logical access (logging on) the client's system.

When accessing your clients, you might have access to your client's information assets, confidential data, or restricted facilities.

assist them to identify you via e.g. photo ID, staff card, wearing name badge and uniform as required

request access (physical or logical) via a formal channel before you go, and they may need to provide tags, keys, or other methods for you to access these areas.

disclose any possible hazards that your service might introduce to your client.

use safety signs or notice to notify people around you.

learn whether the organisation has any special requirements

Security clearance

01

What are the WHS and environmental requirements are you aware of in networking services

02

What are some safety and administrative issue do you need to consider disclosing?

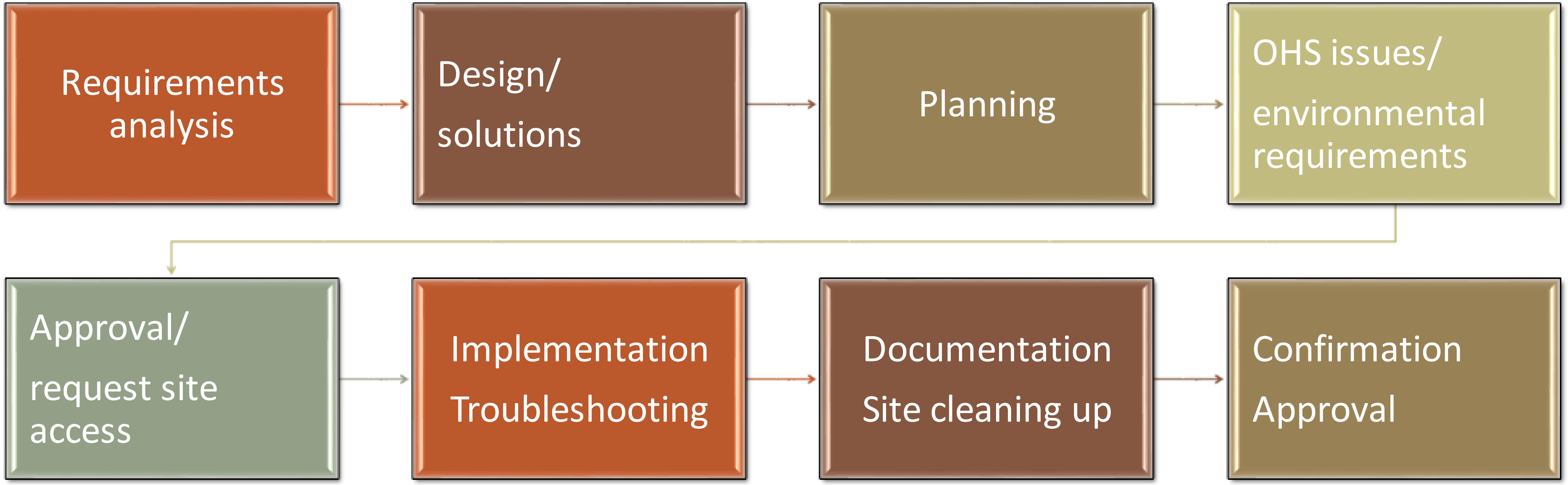
03

How to consulte with the appropriate personnel about the above questions.

Discussion:

Planning for Installation

An framework of IT service lifecycle



Implement enterprise network – relevant tasks

Describe network modelling
- Segments – sub networking
- Topology
- Cross function Connection (inter networking)
- Access control

Determine nature and scope of the network routers and network switches and network resources from job briefs or appropriate personnel

Prepare for given work according to occupational health and safety (OHS) and environmental requirements

Obtain existing operating instructions, manuals, hardware and software requirements

Use a hierarchical internet protocol (IP) network address scheme

Follow the process of configuring switches and routers to enable local area networks (LAN) and WAN links

Use network diagnostic and troubleshooting techniques for troubleshooting network faults and implementing recovery actions

select and use tools and equipment to analyse enterprise networks.

maintain enterprise network documentation

ensure the task is coordinated effectively with others involved at the worksite

The nature and scope of network routers, network switches and network resources

DETERMINE CUSTOMER NETWORKING REQUIREMENTS

Nature of Networking Services

- Installation : could be one-off or ad hoc, this includes assembly individual devices and configure **the functionality, performance parameter, security, and Interoperability.**
- Troubleshooting : typically ad hoc, this includes locate, diagnose, and rectify issues on functionality, **security,** performance, and **Interoperability.**
- Operation : this includes patch, upgrade, maintain, backup, authorization etc. **Typically ongoing.**
- Optimisation: reconfigure devices against the guidelines and user requests. **Typically ongoing.**

Requirements analysis - determine customer networking requirements

The association between business domain and IT frameworks

Business process of an organisation may have direct impact on its information flow

Business domains and organisational structure may determines how the orgasniation set up its network segmentation,

Logical user access control should be largely a reflection of a company's reporting lines and organisational structure.

People within the same business function may have similar information access requirements.

Business areas and services may inform the type of network access methods and traffics.

Example: Specific tasks in network configuration

- **Review system design**
- Contact ISPs, vendors, and Order devices (subject to budget and availability).
- Building prototype or testing bed and verify the solutions.
- **Prepare site access (subjects to approval)**
- Install and configure devices: user edge and test connectivity
- **Install and configure node devices: connections and protocols (subjects to delivery and testing)**
  - Configure ip interfaces
  - Chose the adaptors if necessary, according to the carrier's instructions.
  - Configure vlans and trunking
  - Confiture port sesurity
  - Configure routing protocols
  - Configure access control lists to network services and applications and inbound traffics on the gateway.
  - Configure IP services: dynamic or static IP addressing, IP routing, network address translation (NAT)
  - **Configure redistribution (if involves new adaptor may needs to be turned off)**
  - **Configure router roles (stub)**
- **System testing (may need rollback plan)**
- **Documentation**
- **User training and signing off**
- **ISP billing confirmation**

Consideration of priority and contingency

IP configuration, access control, carrier configuration, which one goes first?

Generally, self-defence needs to be enabled before a device is connected. Some services demands an valid IP address

How and when we will be doing this (Plan)

What to do	Who will do it	When by	How	Outages/contingency	Priority

01

What tasks do you need to include in your installation services

02

How would you determine the order and time frame of these tasks

Discussion:

Asking for approval and communicate with stakeholders

Summary of Preparation tasks

Review WHS, code, guidelines, legislation, standards, and organisational policies that might be relevant to the project.

Review given system design documents, existing configurations, logs.

Validate new configuration (if any) with your client and stakeholders.

Select/recommend models of devices. Collect product information from vendors or clients

Develop configuration checklist and benchmark

Disclose any potential general hazards or hazards associate with telecommunications, RF, and electric devices (page 5)

Conduct OHS/WHS induction (as per XYZ's policies)

Conduct site inspection and make sure it satisfies environmental requirements defined by the vendor or industry body(page 6).

Conduct security clearance with the clients/sub-contractors.

Clarify how client's personal information will be collected and protected(as per page9). Confirm privacy protection strategies/polices

Request site access with details about your job.

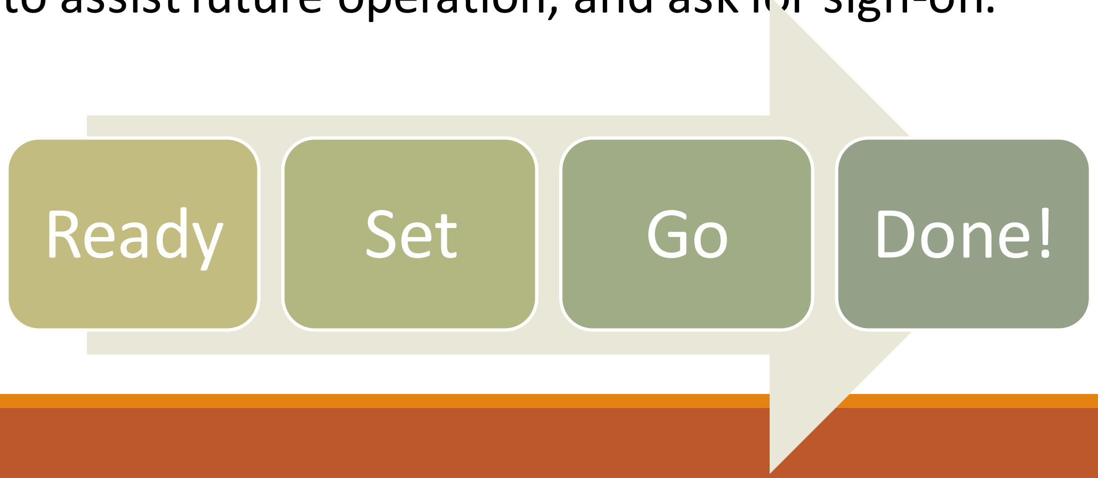
IT service lifecycle - communications

1, Design : knowing what your client needs, making recommendation on the architecture, function, non-function specification, and parameters.

2, Preparation : making action plan, investigate OHS issues, request site access, provide security clearance.

3, Implementation :

4, Testing and signing off : review and specify what have been configured / provide documentation to assist future operation, and ask for sign-off.



Email 1- Asking for information about business requirement

Mr/Ms A:

We would like to know…

- The size of the company, how many staff numbers do they have. How many offices and sites do they have.
- What's their orgasniational structure, how many departments do they have?
- What is the client's core business?
- What enterprise information service do they need (ftp, emails, Samba, web, database, remote desktop, VOIP, video conferencing etc.)
- Do they have specially security concerns.
- What are the regulatory requirements for your industry. …

Regards,

Your name

Email 2- Asking for approval

Mr/Ms A:

- We are going to deliver…
- We will be doing theses things (plan or task list)…
- We would request(site access, resources, powers, guidelines etc.)…
- I refer to (legislation, WHS issues etc.)…
- Some potential issues could be…

Regards,

Your name

Email 3– Asking for signing-off.

Mr/Ms A:

- We have done…

  (task list, function description, system specification)…
- We have provided these documentation and training(if any)
- Some potential issues could be…
- Some expected benefits can be…

Regards,

Your name

Asking for confirmation

System profile and specification,

- Hardware specification and lists,
- Software specification and profile,
- Function descriptions

User manuals,

Training materials

Enterprise features and applications

Enterprise features and applications

- An Enterprise might have established, formal organsiation structure.

This informs the access control and permission of network applications, and network segmentation for the infrastructure. This also determines the distribution of application components. The structure also often determines reporting lines and authorisation.

- An Enterprise might have missions, strategic plans, and explicitly defined business functions that the enterprise operates to achieve the mission:

Business functions are conditioned by different departments. This inform the data sets, user groups, and user access policies.

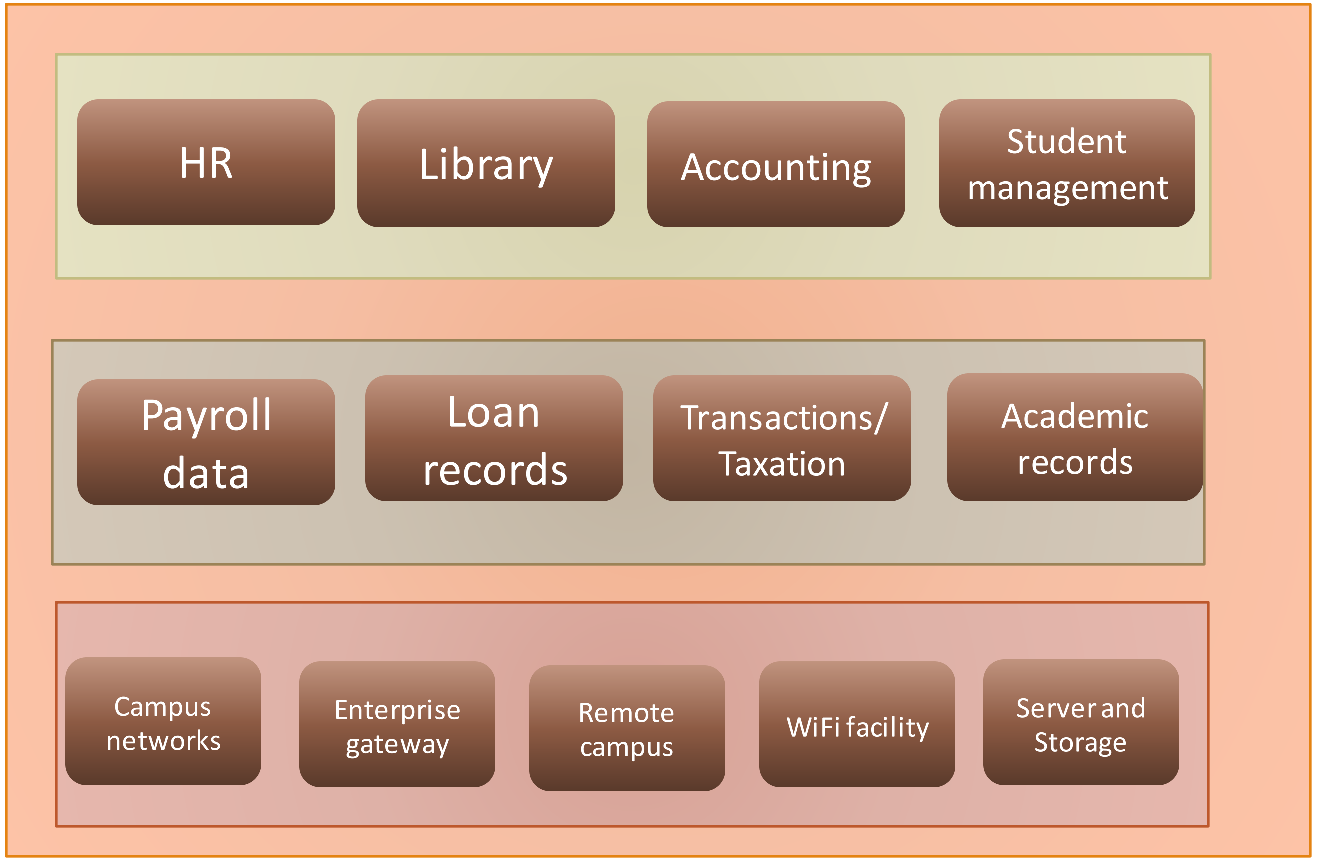
- An Enterprise might have explicitly defined business procedures.

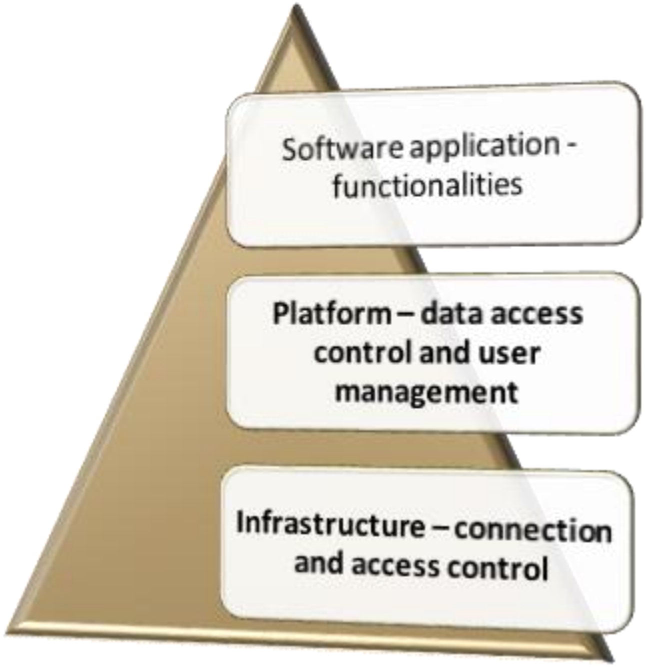
This can be supported by business applications, e.g. Pay roll, CRM(customer relationship management), ERP(enterprise resource planning), AIS (accounting information system), email system (e.g. MS Exchange) etc.

- An enterprise might also subject to regulations and public liability, e.g. free of information etc.

A public web site or web app might be necessary.

Example: Executive view of ICT architecture





Categorise core business asserts and IT asserts

Source: http://www.anao.gov.au/bpg-projectplanning/2_1_2_understanding_of_ICT_strategy.html Retrieved 11/07/2017

Business functions

Production Function

- Research/development
- Production/quality

Supporting/resourcing

- Management
- Admin/HR/finance

Marketing function

- Promotion/distrabution
- Public relationship

Example: record keeping procedure

Note that record keeping is often a legal requirement, and organisations need to ensure their compliance with legal obligations (e.g., Public Records Act 1973 in Victoria).
See a sample here: http://accsa.org.au/wp-content/uploads/2016/10/Record_Keeping_Policy_Safe-Balance.pdf

For enterprise networks, record keeping and documentation helps with change / configuration management and trouble shooting. E.g. you can easily refer to your notes and build existing knowledge database, this will make troubleshooting easier. Documentation also help maintain consistency/compliance, and keep trail of audit. Documentation can also provide better understand the complexity of the system, e.g.: functional and non-functional requirements, system settings, compatibilities, current configuration and system status.

The procedure might include but not limited to the followings steps.

- ❑ Define the purpose, why you want to keep the records.
- ❑ Scope: what you should keep with cclassification to avoid disputes
- ❑ Follow the naming convention, Define Names and types of records that need to be kept (categorisation)
- ❑ Timeline: how long you should keep them for
- ❑ Media and security: Set up access control and authorisation, e.g. how you should keep the record (paper, digital, online) and how to protect the information.
- ❑ Archive and dispose: how you should Archive and remove the information. Define the timeframe of records retention, e.g., five years
- ❑ Version control: how you should name and order the medias if you have multiple version
- ❑ Maintain and audit confidentiality

Record keeping –version control

Version control information

Date stamp

Release logs

Checklists

Other implicit information. New reports.

Security measures

- Vlans –virtual local area networks: this is a logical subdivision of LAN segments. A Vlan is a group of ports that share the same network ID and they are in the broadcasting domain. L2 traffics are restricted within the same broadcasting domain.

Sub-networking can be based on business functions or organisational structure.

- Port security: it defines the expected association between Mac-addresses and L2 ports and the actions to be taken when any association is violated.
- Access control list: there are L2 or L3 (IP) access control lists. They filter traffic based on a number of rules, e.g. source addresses, destination addresses, and protocols.
- Firewall: firewalls filter traffic from L2 to application layer based on rules called "policies", more common firewalls are packet filter firewall (L3), stateful firewall (L4 and L5), application proxy firewall (L3-7, and some appliance can even check the content).

Information for user network access requirements

- The size of the company, how many staff numbers do they have
- How many offices and sites do they have.
- What's their orgasniational structure, how many departments do they have?
- Do they have people work from home.
- What enterprise information service do they need (ftp, emails, Samba, web, database, remote desktop, VOIP, video conferencing etc.)
- Do they have specially security concerns.
- What is the client's core business?

Stakeholders

They might have impacts on your services, especially those who can influence decision-making

They can be affected by your services.

CIO,

IT manager,

IT technicians,

Users/line managers,

OHS officers,

Security officer

Oral communication skills

Listening: active listening: with cues and confirmation, without interfering the speaker. Uses listening and questioning skills to confirm understanding for the requirements, participates in a verbal exchange of ideas/solutions, and uses appropriate, detailed and clear language to address key personnel, and to disseminate information

Uses specific and relevant language to clearly describe and explain, a range of technical, operational and business-related matters.

Interaction: Rephrasing and redirecting.

Qustioning :4 W 1 H

WHO SHOULD I DEAL WITH – KNOWING THE CLIENT

WHAT DO THEY NEED ME TO HELP WITH – THE PROBLEMS AND REQUIREMENTS

WHEN CAN I START AND GET THINGS DONE – THE TIMELINE AND PLAN

WHERE WILL I GET IT DONE – ACCESS THE SITE AND CHECK THE ENVIRONMENT OF THE SITE

HOW MUCH WILL IT COST – THE BUDGET

Further consideration

Is my services regulated under any law/licensing requirements? E.g. do I need a license?

What is the situation of the existing system? E.g. knowing your “patient” before undertaking a “surgery”.

Does the site have suitable environment for my devices? E.g power supply, temperature and humidity.

Will I or my devices or my services cause any hazards to the workplace? E.g. noise, RF.

Do I have permission to access the system? E.g keys or RFID to the datacentre or passwords

01

What do you need to know before your networking installation services?

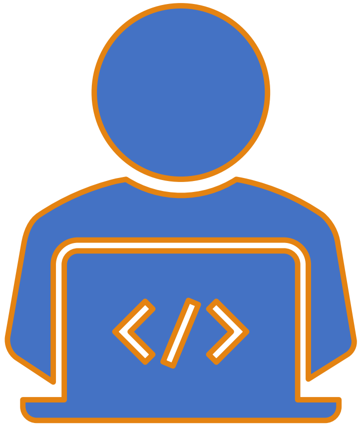
02

How do you determine the networking needs based on enterprise procedures?

03

How do you obtain information about existing documents make sure it is up to date?

Discussion:



Requirements analysis - Select and obtain network services and network application requirements

Evaluate client user requirement

- Number of users,
- Organisation structure,
- Information services,
- Business applications,
- Internet access,
- Data volume,
- Security policies,

Network Design Considerations - Business

- Current problems
- What is needed?
  - Need to send files from A to B
  - Need to store and have access to ……?
  - Need to run software X to do Y
- Locations of sites
- Number of users
- Key Systems and data sets
- Tolerance of down time
- Budget
- Service provider contracts – hardware, software, communications
- Expansion / upgrade plans
- Critical events / times of year

Reliable, flexible and available

What we can do to help business

Job processing

Information gathering

Data storage and processing

Access controls

Network communications

Business processes	Data flow
Business information	Data sets
Communications/access	Network infrastructure

What we will be delivering (specification)

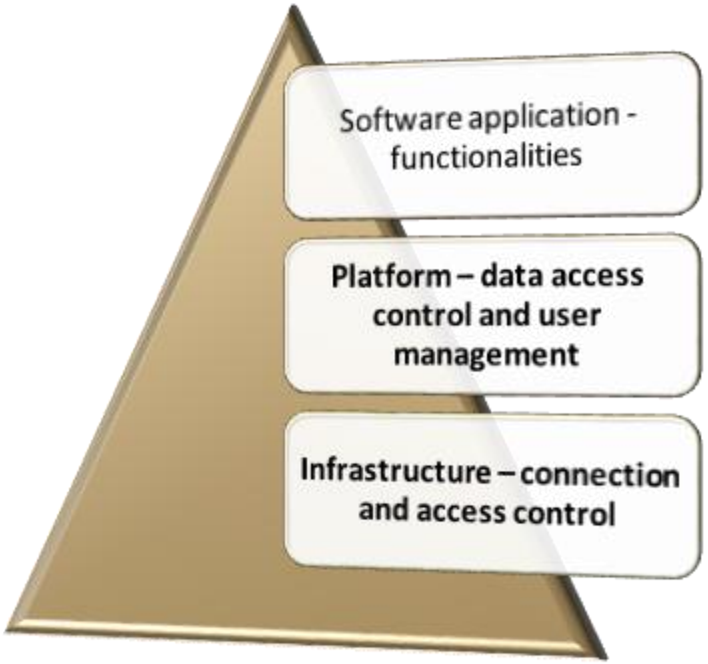
System profile and specification,

- Hardware specification and lists,
- Software specification and profile,
- Function descriptions
- System performance (non-functional) benchmark

User manuals,

Network Hardware and selection -outers, network switches and network resources

System administration –Platform/NOS



Elements of the Network architecture

The path that a message takes from source to destination:

as simple as a single cable connecting one computer to another, or as complex as a network that literally spans the globe

A enterprise network architecture include the logic structure of network elements and how they provide connection and maintain the contact.

The network infrastructure contains three categories of network components:

- End devices
- Node/Intermediary devices
- Network media

Summary of Network elements

- Node Devices: models, adaptors, connections and protocols,
- Edge devices: user edge, carrier edge (ISP)
- User devices and terminals
- Management devices
- WAN links (Frame Relay, ADSL, DDN, X.25, FTTN+LAN)
- Internet access (ADSL, PPPOE)

- IP services: dynamic or static IP addressing, IP routing, network address translation (NAT)
- VPNs (IP sec, GRE, SSL etc)
- Access control and edge security.

Network Design Considerations - Technical

- Number of sites
- Number of users (total and per site)
- Current topology
- Communication Options between sites
- Network / Server Availability
- Bandwidth Requirements / available
- Latency – voice / applications
- Redundancy – cost of downtime?
- Internet Link Redundancy
- Security – firewall / VPN / Encryption / Remote Access
- Quality of Service – Voice / "sensitive applications"
- Existing building / campus cabling
- Space – cabinets, racks, power,
- Security – firewall, authentication, encryption, remote access, subnets, access control lists, wireless
- Cost / Budget

Network software applications

Web browsers: Google Chrome, Mozilla Firefox, Opera, Microsoft IE and Edge, Apple Safari

Email clients : Thunderbird, Outlook, Gmail, Evolution.

Instant messaging : Skype, Facetime, Whatsapp etc.

Collaboration Applications : Team View, Cisco Webex, Openmeeting (Apache)

Business applications : SharePoint, Salesforce CRM, Sage ERP

01

How does your client’s business function and organisational structure determine your networking solutions?

02

How would you obtain and read product specification?

03

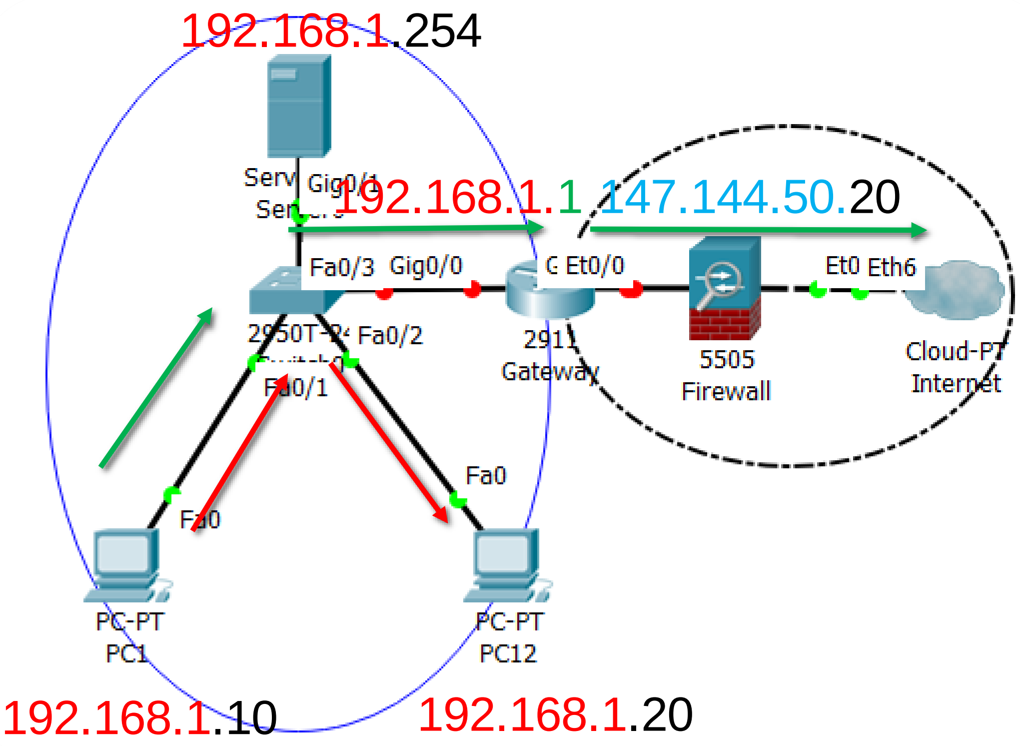
What network elements do you need to include to support your clients networking requirements?

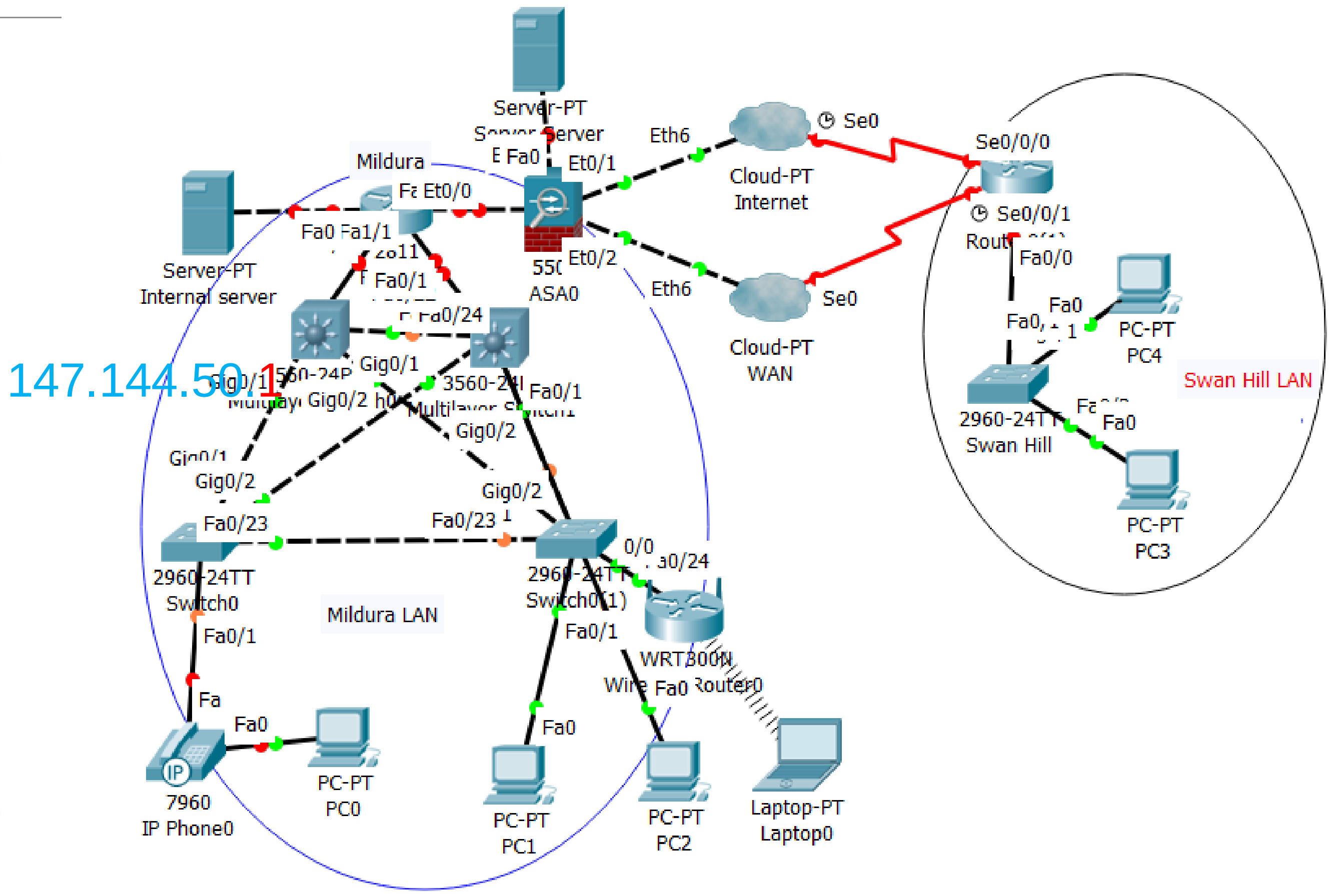
Discussion:

Network Architecture Models

- A Network Architecture Model can be a reference model that describes a hierarchical structure that consists of multiple layers of protocols, hardware, and software needed to transmit data between two hosts or devices.
- A shared reference helps with different components or different manufacturers’ products to be connected by converting signals to the agreed form, e.g. IoT.
- Network modelling is the way how network components (e.g., devices, node, protocols, and connections) can be classified, categorised, and logically presented. Open Systems Interconnection (OSI) Model, and Transmission Control Protocol/Internet Protocol (TCP/IP) Model

Intranetwork - Internetwork





How networking enables devices to talk - Protocols

The concept of networking

The concept of protocols

The concept of internetworking

The concept of enterprise system

70

Summary of Networking technologies (LAN, WAN, Firewalling, etc)

Protocols

"a: a code prescribing strict adherence to correct etiquette and precedence (as in diplomatic exchange and in the military services)

b: a set of conventions governing the treatment and especially the formatting of data in an electronic communications system"

https://www.merriam-webster.com/dictionary/protocol

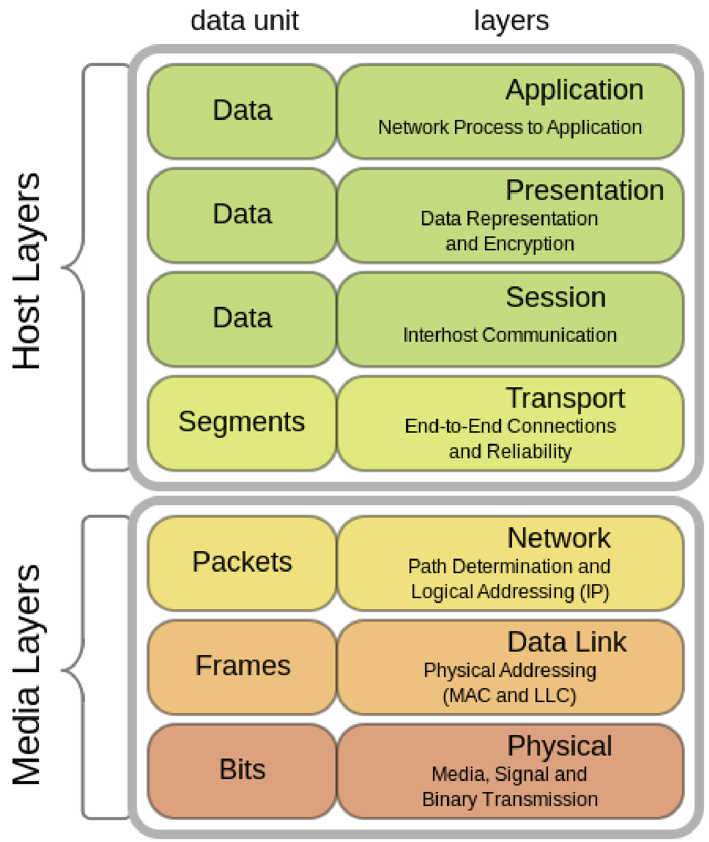
- Enables communication – how we communicate
  (convention used for establishing transmission rules)
  - When
  - Where
  - How
    - In what language
    - In what manner
  - With whom

Communication between different devices

- Communication between two computers
- Communication between you and your computer

Jonas Stocker, 2018, Astronaut meeting Alien.png - Wikimedia Commons, URL: https://commons.wikimedia.org/wiki/File:Astronaut_meeting_Alien.png retrieved on 05/09/2023

The 7 Layers of the OSI Model



The **OSI** or **O**pen **S**ystems **I**nterconnection model defines a networking framework for implementing protocols in seven layers.

Connections are established at different level – from more "basic" to more "sophisticated".

The **OSI** or **O**pen **S**ystems **I**nterconnection model defines a networking framework for implementing protocols in seven layers.

Connections are established at different level – from more "basic" to more "sophisticated".

Source:Français, 2019, CultureDuQ on WikiCommons, URL: https://commons.wikimedia.org/wiki/File:OSI_Model_v2.svg retrieved on 05/09/2023

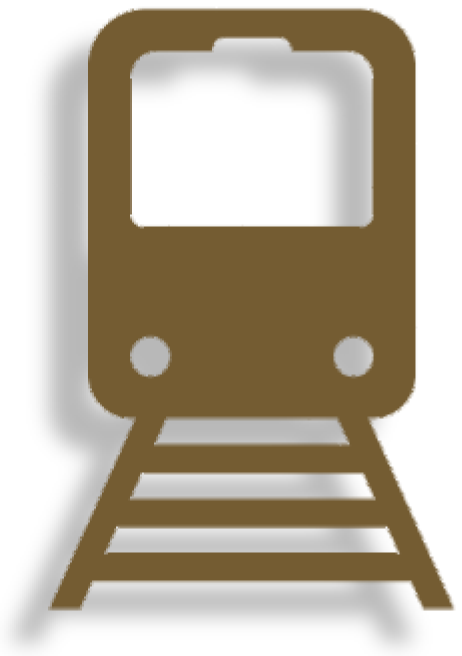
ISO/OSI L7 to L5 - diplomatic formality, precedence, and etiquette

L7: Provides user applications interfaces for network services and end users, e.g. mail, http, ftp, telnet, DNS

L6: defines the conversion, format, encryption, compression for data transfer, e.g. JPG for images, html for web pages, ASCII text for documents.

L5: determines how a connection is two devices is established, maintained and managed, and this may also include how different sessions are coordinated and secured.

ISO/OSI L1 to L3 – “building roads”



L1: Specifies:

- how data is processed into bits;
- how bits are reconditioned and reshape into signals (electronic, RF, lights etc.)
- how singles are synchronised, physically transferred over medium, such as cables, unshielded twisted pairs (UTP), Fibre optic, Wi-Fi etc.

L2: establishing and maintaining data communication links, encaptualising packets into frames (the Protocol Data Unit -PDU), detecting and correcting transmit errors, handling physical addressing (MAC).

L3: Responsible for establishing routes to research different hosts and networks based on Internet protocol (IP) addressing and the information stored in the routing table. It also manage network traffic congestions through time to live (TTL) information. Packet is the (PDU) at L3.

ISO/OSI L4 – “establishing rules “

This is the layer for “traffic control” with designated “lanes” (ports) etc.

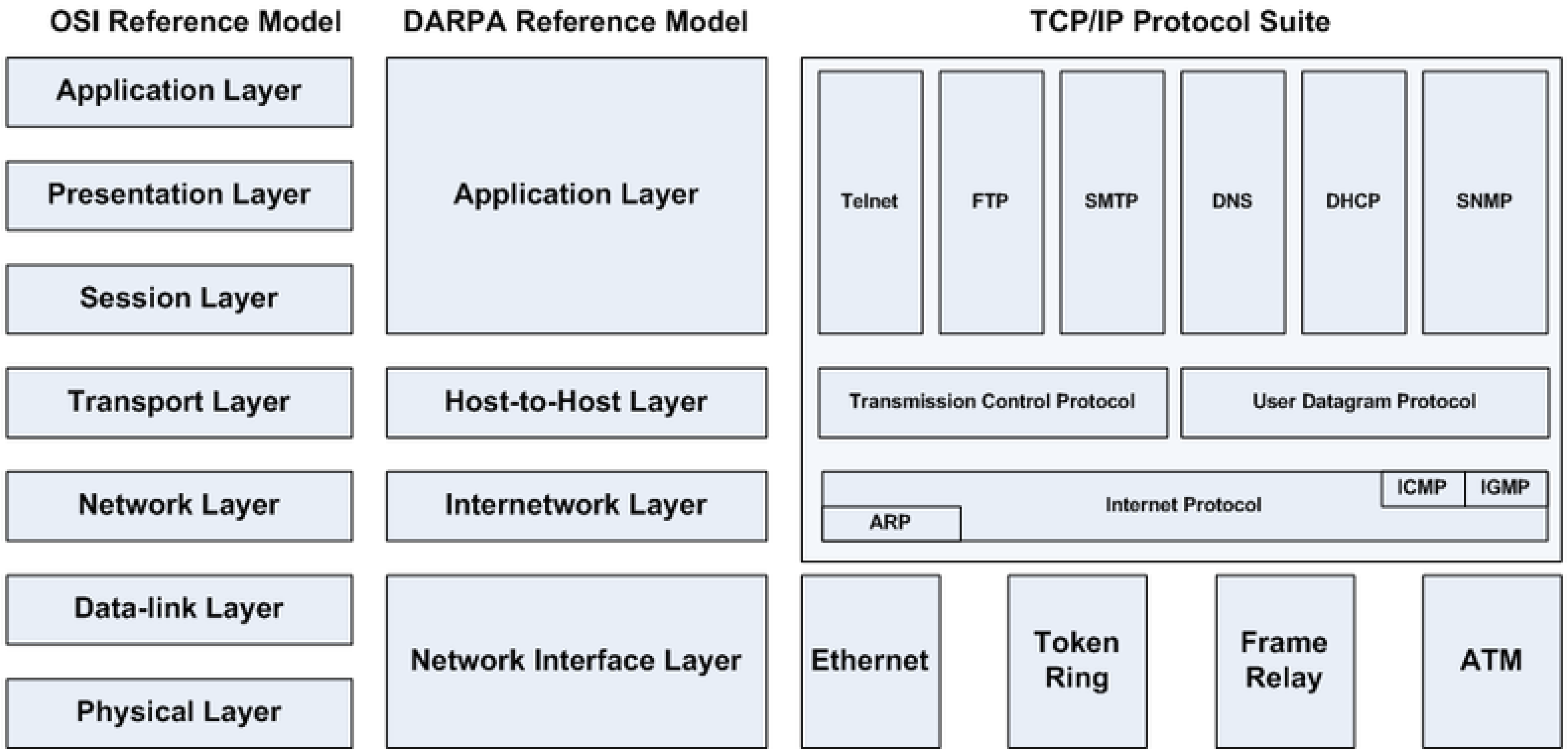
It creates data segments, establishes end-to-end logical connections and flow control by adjusting the window size (using handshake methods) .

There are two transport protocols:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP).

This layer also has error handling and packet assembly functions.

TCP/IP and OSI model.



The TCP/IP model is a guideline of specific networking protocols to enable computers to communicate over a network.

TCP/IP functionality is divided into four layers, each with its own set of agreed-upon protocols.

Source Lihat di bawah. URL:https://id.wikipedia.org/wiki/Berkas:OSI-DARPA-TCP.png Retrieved on 05/12/2017

TCP/IP Protocol Suite

The TCP/IP model is a description framework for computer network protocols created in the 1970s by DARPA.

It evolved from ARPANET.

The TCP/IP model is a guideline of specific networking protocols to enable computers to communicate over a network.

Examples of protocols (L1-L2)

Layer 1 protocols (Physical Layer)

- ADSL Asymmetric digital subscriber line
- Leased line: T-carrier (T1, T3, etc.) or E-carrier (E1, E3, etc.)
- ISDN Integrated Services Digital Network
- RS-232

Layer 2 protocols (Data Link Layer)

- IEEE 802.3/8/11/14/15/16

e.g. Ethernet .3, WiFi .11

- CDP Cisco Discovery Protocol
- FDDI Fibre Distributed Data Interface
- PPP Point-to-Point Protocol
- PPTP Point-to-Point Tunnelling Protocol
- STP Spanning Tree Protocol

Examples of protocols (L2.5-L3)

Layer 3 protocols (Network Layer)

- IPv4 Internet Protocol version 4
- IPv6 Internet Protocol version 6
- ICMP Internet Control Message Protocol
- IGRP Interior Gateway Routing Protocol
- IPSec Internet Protocol Security
- IPX Internetwork Packet Exchange

- OSPF Open Shortest Path First
- EGP Exterior Gateway Protocol
- BGP Border Gateway Protocol
- RIP Routing Information Protocol
- EIGRP Enhanced Interior Routing Protocol

Examples of protocols.

Layer 4 protocols (Transport Layer)

TCP Transmission Control Protocol

UDP User Datagram Protocol

GRE Generic Routing Encapsulation for tunnelling

Layer 5 protocols (Session Layer)

SMB Server Message Block

NFS Network File System

Knowledge domains

Traffic control	**Transmission Control Protocol**	Connection	3-way handshake and windows	**Port ID**
Across networks (inter-networking	**Internet protocol**	Routing	(**Gateway**)	**IP address**
Local network (intra-network)	IEEE 802.3	Switching	Broadcasting	Mac address

TCP

Traffic control

Transmission Control Protocol

Connection

3-way handshake and windows

Port ID

TCP

Transmission Control Protocol/Internet Protocol (TCP/IP) work together as a set of networking protocols connect two or more computers to communicate.

TCP is a typical connection-oriented protocol.

TCP uses a three-way handshake to **establish** a **connection**,

A port is an endpoint to a logical connection, which represents a certain network service

Network services and port IDs

21 FTP (File Transfer Protocol)

23 Telnet

25 SMTP (Send Mail Transfer Protocol)

53 DNS (Domain Name Service)

68 DHCP (Dynamic Host Control Protocol)

80 HTTP (HyperText Transfer Protocol)

110 POP3 (Post Office Protocol, version 3)

137 NetBIOS-ns

138 NetBIOS-dgm

139 NetBIOS

143 IMAP (Internet Message Access Protocol)

TCP/IP cont…

As a non-proprietary protocol suite, Transmission Control Protocol/Internet Protocol are now the most commonly supported. It was based on the Defense Advanced Research Projects Agency (DARPA) Internetwork.

TCP and IP work together as a suite of communication protocols used to interconnect network devices, it is the foundational protocol of the internet.

They provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination.

TCP: responsible for connection and the data delivery of a packet, handles communications between hosts. It supports flow control, multiplexing and reliability. TCP establishes connections between the sender and receiver with both IP addresses, port IDs. It provides reliable data transmission and packet assembly via sequencing, acknowledgement, error check, and error recovery.

IP : defines for the logical addressing and routes to the destination

Examples of protocols (Application Layer)

- Port 21 - FTP, File Transfer Protocol
- Port 22 - SSH, Secure Shell
- Port 23 - Telnet, a remote terminal access protocol
- Port 25 - SMTP, Simple Mail Transfer Protocol
- Port 53 - DNS, Domain Name System
- Port 67/68 - DHCP, Dynamic Host Configuration Protocol Port 546-547 DHCPv6
- Port 69 - TFTP, Trivial File Transfer Protocol, a simple file transfer protocol
- Port 80 - HTTP, HyperText Transfer Protocol
- Port 110 - POP3 Post Office Protocol Version 3
- Port 123 - NTP, Network Time Protocol
- Port 135-139, 150 - NetBIOS, Fie Sharing and Name Resolution protocol - file sharing with Windows.
- Port 143- IMAP, Internet Message Access Protocol
- Port 161-162 - SNMP, Simple Network Management Protocol
- Port 389 - LDAP Lightweight Directory Access Protocol
- Port 500 – IP sec Virtual Private Network (VPN)
- Port 860 –iSCSI
- Port 902-- Vmware Server
- Port 1812-1813 - RADIUS, an authentication, authorization and accounting protocol

VOIP

Transmitting voice over IP networks.

H.323 Provides interoperability

H.225 Call signaling and registration

H.245 Negotiates the usage of the media channels

SIP IETF standard for providing voice over IP

MGCP Gateway protocol that defines communication between the call agent and the signaling gateway

RTP Provides real-time transport over packet switched networks

RTCP Control protocol that provides feedback to the application

RSVP Responsible for providing QoS by reserving resources

RTSP Provides control over delivery of real-time media streams

https://www.cse.wustl.edu/~jain/cis788-99/ftp/voip_protocols/index.html

01

What do you need to build a network architecture

02

Why do we need protocols, and port IDs?

03

Compare LAN and WAN, Intranetworking and internetworking, TCP and IP.

Discussion:

Connect enterprise LAN and WAN

LAN - Local Area Network

- A LAN connects network devices (computers or electronic devices) within a relatively short distance, LAN can be a logical concepts, e.g. virtual LANs.
- A LAN might be in one single switch or span a group of switches through trunking (Interswitch connections).
- In TCP/IP networking, a LAN is often implemented **as a single IP subnet (same network ID)**
- A LAN is normally within the same **broadcasting domain.**
- LAN is normally associated with **a certain orgnistional unit or user group**.
- **Ethernet is a common connectivity technologies**

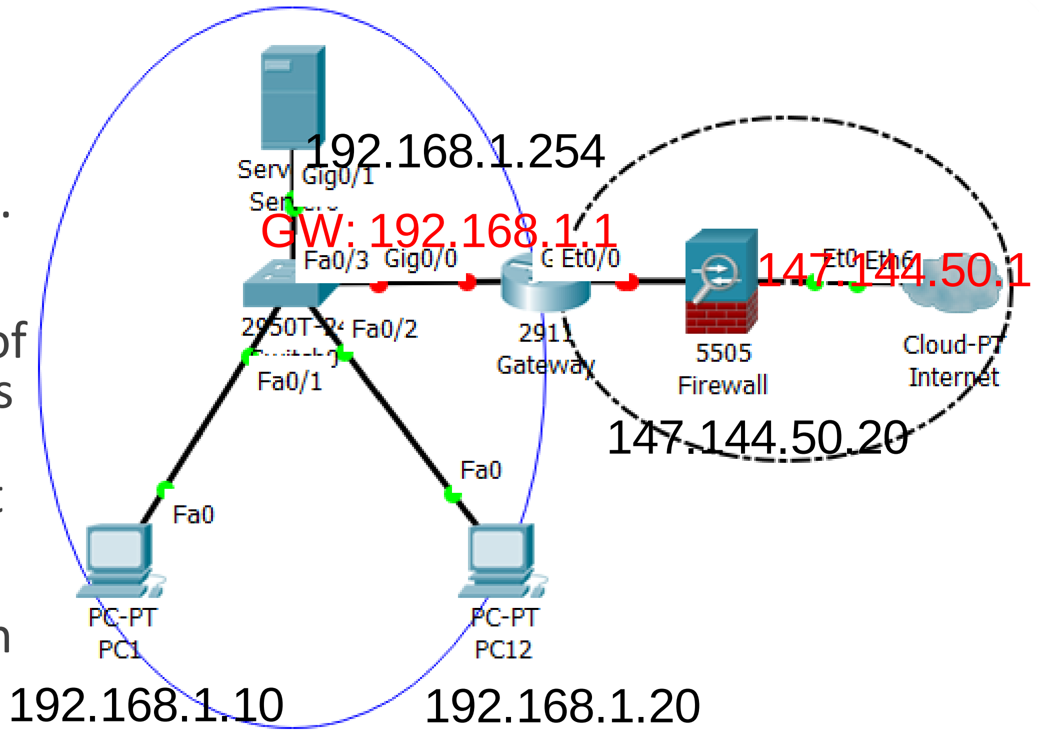
Internet Gateway

Each LAN has its own internet gateway. Local hosts can access the gateway directly (from 192.168.1.10 to 192.168.1.1 via the switch), and the gateway (the router) can then go the other networks (147.144.50.1). Normally this is role is played by a router:

When the switch sees that the destination IP address of a packet is in a different network, the switch first sends the packet to the gateway router interface rather than any local computer. The gateway can further forward it to another external-facing interface.

Note that a router might have multiple interfaces, each interface can be the gateway of a LAN.

Gateway can be called as default router, but for a certain LAN, "gateway" address refers to the address of the single interface connected to that local network.



Gateway– the “post office”

A routing interface (not the whole router) for a LAN is called a gateway interface for that LAN. Different LAN has their own gateway interface, and it is accessible by its local computers, this means it has an interface that belongs to that local network.

Computers in the same LAN have the same network ID, in this case a switch can forward the traffic differently to the destination host.

However, computers in different networks have different network IDs.

When a packet goes to a remote destination (in a different network and the destination IP address has a different network ID), the switch simply forwards it to the gateway interface. In this case, the initial destination Mac address is the gateway’s address despite that the destination IP address is in a different network.

WAN - Wide Area Network

- A WAN is a collection of geographically(or logically) distributed LANs.
- A WAN is a typical **internetworkin**g instance as it spans a large physical distance, e.g. the Internet. However, modern WAN technologies might help connect hosts in the same logic segment through different virtual links (e.g. VPNs, L2 MPLS) .

- A WAN might have multiple broadcasting domains.
- They also tend to use different technology like FTTX+LAN, SDH, DDN, ATM, Frame Relay , ADSL, ISDN and microwave for connectivity over the longer distances.
- VPN (virtual private networks) over the internet has become more popular than ever as a WAN solution.

WAN technologies

<u>Some WAN services might not simply classified as Layer 2 or 3 protocols</u>

- MPLS Multi-protocol label switching, a technology routing technique in telecommunications networks that directs data from one node to the next based on short path labels. MPLS uses label-switched path (LSP).L3 MPLS VPN works with vrf (virtual routing and forwarding).
- X.25 a packet-switching WAN technology
- ATM Asynchronous Transfer Mode
- Frame relay, a simplified version of X.25 create virtual circuits (e.g. PVCs or SVCs) to connect remote LANs to a WAN. Frame is the PDU of frame-relay and it can be forwarded based on map.

Note these protocols are not fully mapped to a single layer of OSI but mainly operate at one of these two layers.

Process for connecting WAN services and applications

Determine WAN technology, interfaces, protocols and performance parameters (e.g. frame-relay, ADSL, FTTX+LAN, etc).

Determine connection requirements, e.g. geographic features. Whether the organisation has multiple sites, and how far are these sites to each other.

Determine traffic and applications, whether they use video conferencing, streaming, VOIP, and some other services.

Determine security and cost expectation, this help choose the most cost effective service without comprising security.

Contact service providers and determine availabilities and costs, compare and review their reputation, pricing, and temrs.

Determine protocols and parameters. (e.g. Ip addresses, protocols etc.)

Confirm terms and installation plans.

Installation and test WAN links and devices

Process of configuring switches and routers for LAN and WAN

For switches:

- Configure virtual local area networks (VLANs) on switches to meet network segmentation requirements
- Configure hierarchical addressing over virtual local area networks (VLANs)
- Configure Inter-Vlan routing
- Configure trunking for inter-switch connection,
- Configure port security, and other LAN security mechanisms (if needed)
- diagnose and rectify network hardware and device configuration faults
- document configuration information, fault-finding history and remediation action.

For routers:

- Configure ip interfaces, Chose the adaptors if necessary, according to the carrier's instructions.
- Configure routing protocols
- Configure access control lists to network services and applications and inbound traffics on the gateway.
- Address other security issues though authentication, encryptions, and zoning, .
- Configure network address translation (NAT)
- Diagnose and rectify network hardware and device configuration faults
- Document configuration information, fault-finding history and remediation action.

Security across networks

Security issues for users within the same local area network:

- Confidentiality: everyone on the public network may see your datagram.
- Authenticity: whether the datagram is sent from the one who claims who is.
- Authorisation: whether the datagram should be responded.
- Integrity: whether the message has been modified during the transmission.

For example, security measures for local network can include but not limited to:
Determine access requirements

Setup secured login including authentication.

Configure the access control lists (ACLs)

Configure port security

Configure firewall policies

Evaluate client user requirement

- **Business architecture** *domain* –
- describes how the organisation's structured (e.g. Marketing, HR, Accounting, Admin, customer services),
- and their business functionality that delivers the mission and strategy of the organisation (e.g. Market development, internal business services, internal control etc.), .
- **An understanding of an organisation's structure and functions, as well as how they interact, is essential for the organisation to be efficiently supported by available technology. It is also important to be able to investigate and select technology to support the organisation's goals.**

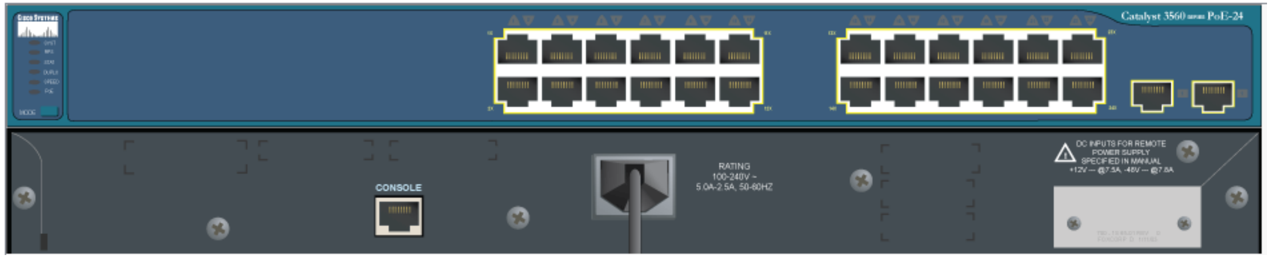
System functions

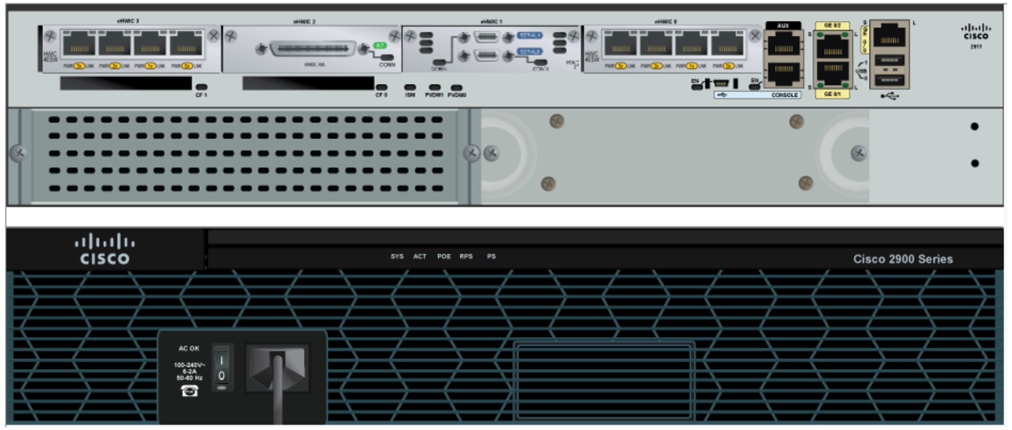
Device	Routing	Switching
Protocols and functions	Based on IP, connecting different networks.	Based on IEEE802, connecting different hosts in the same network (expect for vlans)
OSI layer	Mainly Layer 3 (and above)	Layer 2 (expect for multi-layer switches)
Traffic forwarding mechanisms	Maintain ip route table	Maintain Mac-address table
How to learn paths	Rely on Multicasting	Rely on Broadcasting
Data unit	Forward packets	Forward frames
Operation	Establish routes To a remote destination,	Establish data-link to a local destination,
Network IDs	Source and destination IP address have Different network IDs	Source and destination IP address have Same network ID
Domains	Split/Connect Broadcasting domains	Build broadcasting domains
Examples	Gateway (for WAN)	Bridge (for LAN)

Outline of
Network elements

Categories	Examples
Node Devices:	Routers , switches, bridges, (models), adaptors, connections and protocols,
Edge devices: user edge/carrier edge (ISP)	Modems, waveguides, DTU - data terminal unit
Access network:	ADSL, PPPOE, 3G(WCDMA)/4G(LTE)
WAN links	Frame Relay, ADSL, DDN, X.25, FTTN+LAN), VPNs IP sec, GRE, SSL etc
IP services	dynamic or static IP addressing, IP routing, network address translation (NAT)
Access control and edge security:	L3/L4/L7 firewalls and IDS/IPS
Network servers and controllers:	Windows/Linux/Unit servers
User devices:	Computers, IoT devices, phones, tablets

Sourcing Devices





Networking device: vendors and brands

Cisco

Juniper,

Riverbed,

HP,

Vmware,

Huawei,

NetScout,

Extreme Networks,

Dell

Tp-Link

https://www.openpr.com/news/1279026/Global-Networking-Products-Market-Comprehensive-Study-2018-2025-Cisco-HP-Juniper-Huawei-Arista-VMware-Riverbed-NetScout-Extreme-Networks-Dell.html

Obtain system specifications and availability of system components.

- Vendors' website and knowledge centre
- Vendor and its distribution channel.
- Respectful local retailers.
- Official user manual/handbook.

Families/series

Branch Routers

Cloud Connectors

Data Center Interconnect Platforms

Industrial Routers

Mobile Internet Routers

Network Functions Virtualization

Service Provider Core Routers

Service Provider Edge Routers

Service Provider Infrastructure Software

Small Business Routers

Virtual Routers

WAN Aggregation and Internet Edge Routers

Switch functions and Connecting to the Network

Installation guidelines:

Guidelines for Connecting Ports

Connecting a Console to the Switch

Connecting the Management Interface

Creating the Initial Switch Configuration

Connecting Interface Ports to the Network

Connecting a Fiber-Optic Cable to a Transceiver

Disconnecting Optical Ports from the Network

Maintaining Transceivers and Optical Cables

A list of typical switch configuration steps for LAN and WAN:
Configure your (VLANs) on the switches to meet the network requirements

Configure the hierarchical addressing over (VLANs)

Configure Inter-VLAN routing protocols

Configure trunking

Configure the port security, and any other LAN security devices you need

Other Security measures, such as port security.

How to obtain technical documentation

Vendors’ websites

Product packages

Distributor’s websites

Switch specifications

Displaying Information About Installed Hardware Modules

Displaying the Hardware Inventory for a Switch

Displaying the Backplane and Serial Number Information

Displaying Environmental Information for a Switch

Displaying Temperatures for Modules

Connecting to a Module

Saving the Module Configuration

Displaying Power Usage Information

Power Cycling a Module

Rebooting the Switch

Overview of Supervisor Modules

Overview of I/O Module Support

Overview of Fabric Module Support

Power Modes Overview

Overview of Fan Trays

Router specifications

Connector and Cable Specifications

Connector Specifications

RJ-45

Mini-SMB

MT-RJ

LC

SC-Type

Gigabit Interface Converters

WS-G5484

WS-G5486

WS-G5487

Dense Wavelength Division Multiplexing (DWDM) GBIC Transceivers

Technical/installation requirements

- e.g. Nominal voltage: AC ***-***V
- Operating Temperature: ** °F-*** °F
- Humidity Range Operating ** - **%
- Need to transfer firmware from a local ftp server .
- Need to have a CF card reader

Performance parameters

Portable Product Sheets – Routing Performance

http://www.cisco.com/web/partners/downloads/765/tools/quickreference/routerperformance.pdf

Portable Product Sheets – Switching Performance

http://www.cisco.com/web/partners/downloads/765/tools/quickreference/switchperformance.pdf

Packets Per Second (PPS)

Other:

http://btbusiness.custhelp.com/app/answers/detail/a_id/11094/~/what-are-the-technical-specifications-of-the-cisco-2950-switch%3F

http://www.globalspec.com/specsearch/SearchForm/Communications_Networking/Networking_Equipment/Network_Switches

Summary of Network elements 1

- Adaptors: RJ45 / GBIC / SPF / WIC / Fibre
- Connections and protocols,
- Edge devices: user edge, carrier edge (ISP)
- User devices and terminals
- Management devices

- IP services: dynamic or static IP addressing, IP routing, network address translation (NAT)
- VPNs (IP sec, GRE, SSL etc)
- Access control and edge security.

Summary of Network elements 2

Categories	**Examples**
Node Devices:	Routers , switches, bridges, (models), adaptors, connections and protocols,
Edge devices: user edge/carrier edge (ISP)	Modems, waveguides, DTU - data terminal unit
Access network:	ADSL, PPPOE, 3G(WCDMA)/4G(LTE)
WAN links:	Frame Relay, ADSL, DDN, X.25, FTTN+LAN), VPNs IP sec, GRE, SSL etc
IP services:	dynamic or static IP addressing, IP routing, network address translation (NAT)
Access control and edge security:	L3/L4/L7 firewalls and IDS/IPS
Network servers and controllers:	Windows/Linux/Unit servers
User devices:	Computers, IoT devices, phones, tablets

Devices (you may add lines if there are multiple devices of the same type)	Brand and models/versions	Vendor's contact information	Specification e.g. dimensions, ports, key protocols supported, bandwidth	Prices
Router				
Router firmware				
Switch				
Operating system				
Server				

Network element recommendation

01

You have a router and a switch, which devices mainly work at layer 2, which mainly work at layer 3?

02

How switches and routers work together to build a network for your client?

03

When you see cat5e crossover, UTP, what does this mean?

Discussion:

Network cables

BY CHRIS ZHONG: 2020

Configure IP networks

Application of IP protocols – key steps

- Sub networking: defining/dividing network sizes and address scopes based user nubmer
- Addressing: select the right subnet mask, gateway address, and DNS address
- Address distribution: static IP address or DHCP
- Internetworking: configure Internetworking including intervlan routing.
- Fliting and access control: configure access control lists.

Summary of tasks: configure, verify and troubleshoot routing protocols

- ❑Analysis network segmentation and review existing configuration.
- ❑Design addressing scheme,
- ❑Determine protocols
- ❑Define protocol parameters (e.g. areas, process IDs, autonomy system),
- ❑Emulate existing network and test the interoperability of configuration.
- ❑ Debug and document configuration.
- ❑ Establish baselines
- ❑ Check misteach with given segmentation (unit test) and check connection from end to end (integration test).
- ❑ Using substation or other strategies to fix any issues identified.

Initial (basic) configuration

Look at Resource : http://and discuss:

www.cisco.com/c/en/us/td/docs/routers/access/1900/software/configuration/guide/Software_Configuration/routconf.html#15062

configure terminal

hostname name

enable secret password

no ip domain-lookup

And ssh/telnet,

log,

authentication,

ntp,

I/O memory allocation

Banner

Vlan interface

Backing up IOS and configuration

IOS file system (IFS): reflect your Linux knowledge and some new commands, e.g. show file system.

Make your router a tftp server or use 3rd party tftp router on a PC/server:

tftp-server flash[*partition-number*:]*filename1* [**alias***filename2*] [*access-list-number*]

copy tftp flash

copy running-configuration tftp

show flash

Basic router security and SSH

enable secret 5 (MD5 Hashed Password)

E.g. enable secret 5 cisco123

username admin privilege 15 secret 5 (MD5 Hashed Password)

line vty 0 4

login local

transport input telnet ssh

Learning activity

Research the automatic configuration of one router, analyse these configuration items and the initial value of their parameters.

Change the default configuration of security settings, including at least enable, aaa, ssh.

Setup a tftp server and then back up and restore the IOS firmware and start-up configuration.

Example

username admin priv 15 secret cisco12345

!

aaa new-model

// turn on aaa service

aaa authentication login default local

!

line vty 0 4

Password cisco

transport input ssh

login authentication default

DHCP

Service dhcp

Router(dhcp-config)# ip dhcp pool name
Router(dhcp-config)#network network-number[mask | /prefix-length]
Router(dhcp-config)# domain-name domain
Router(dhcp-config)# dns-server address [address2 ...address8]
Router(dhcp-config)# default-router address [address2 ...address8]
Router(dhcp-config)# lease {days[hours][minutes] | infinite}

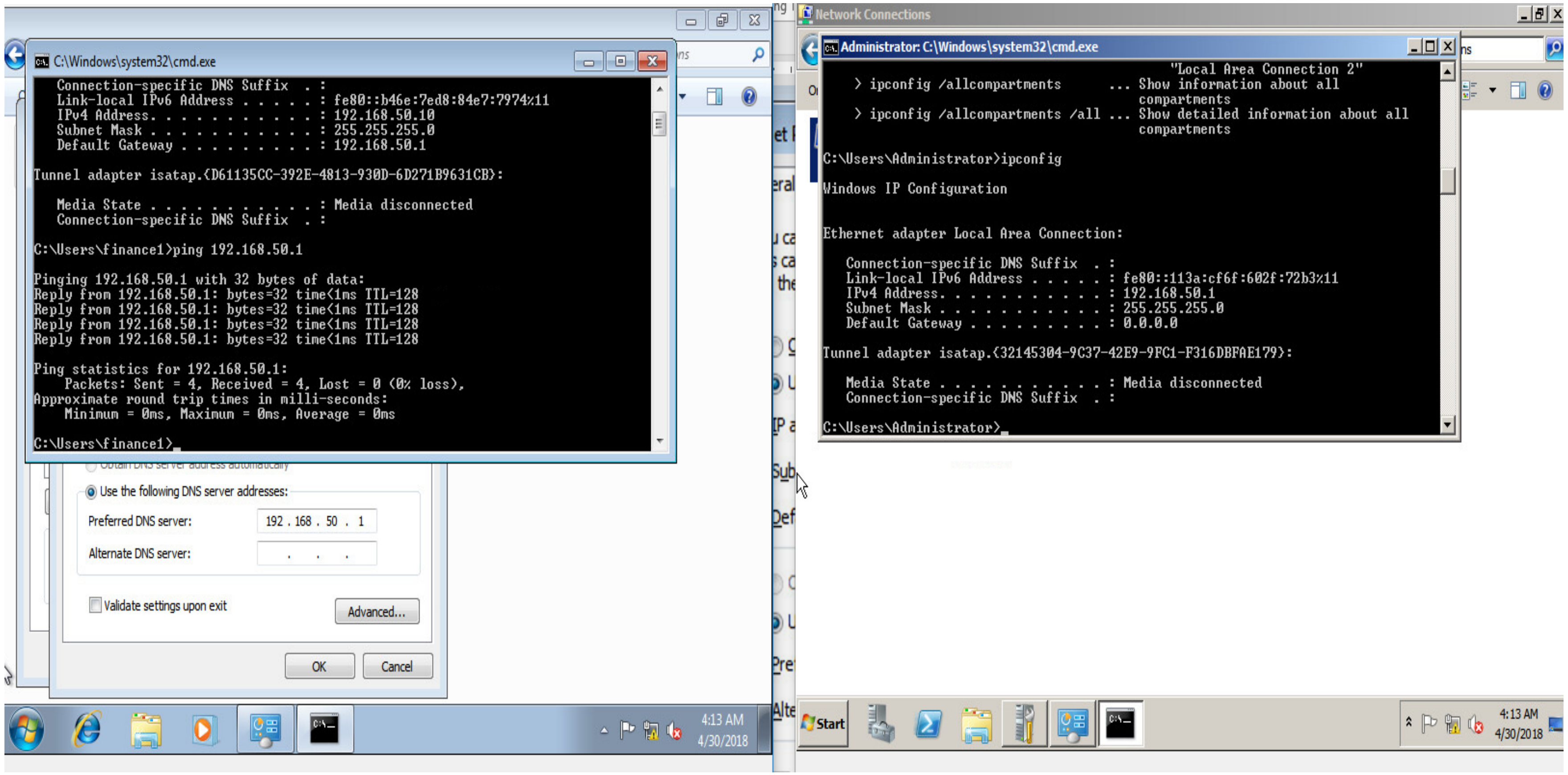
Dynamic IP addressing

Benefits of Using DHCP

DHCP reduces the complexity and amount of administrative work by using automatic TCP/IP configuration:

- IP addresses are supplied automatically
- Correct configuration information
- Many network addressing problems are avoided with consistency

Testing connection - ping



DHCP on the router

Ip dhcp pool POOLNAME

Network 192.168.1.0 255.255.255.0

Default-router 192.168.1.1

Ip dhcp exlude-ipaddress 192.168.1.1

Show ip dhcp pool

Show ip dhcp binding

01

What does an ip addressing scheme involve?

02

How can you use DHCP server to create hierarchical addressing ?

03

When you see cat5e crossover, UTP, what does this mean?

Discussion:

Basic routing

A router is able to connect two or multiple different networks

A router has a routing table (comparing to Mac-address table in switching’s case)

A routing determines where it should forward traffic from a network to other network based on its routing table

Check routing table:

Show ip route

Learning outcomes

- How does a router know where it should forward data to?
- How does a router build and store its knowledge about the location of each hosts?
- A router has three interfaces, how do you know which one is your network’s gateway?

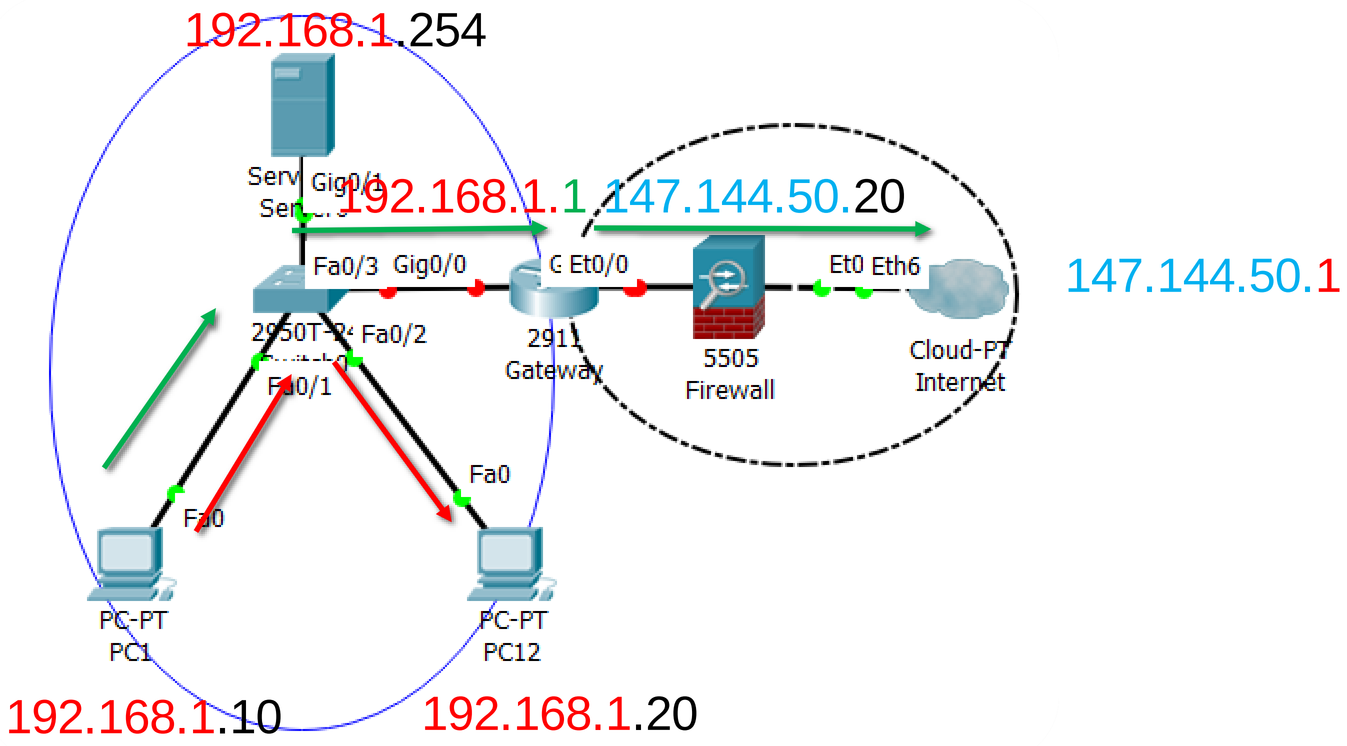
Routing network architecture

Network architecture - the devices, connections, and products that are integrated to support the necessary technologies and applications (Source: Cisco, Introduction to Networks: Exploring the Network http://www.ciscopress.com/articles/article.asp?p=2164577&seqNum=8cations.)

There could be multiple routes but routers will determine the best paths based on different metrics.

The actual logical networks is determined by the route selection.

Internetworking and intranetworking



Internetworking and routing

A wide area network consists of LANs that are geographically distributed. Normally computers across different LANs can only reach each other with telecommunication circuits.

Logically, communication across LANs is an internetworking scenario. A router can be used to connect multiple LANs. Rorters use routing protocols to determine the route and next hop to a remote destination.

A routing interface (not the whole router) for a LAN is called a gateway interface for that LAN. Different LAN has their own gateway interface, and it is accessible by its local member computers.

Computers in the same LAN have the same network ID. But computers in different networks have different network ID

Across networks (internetworking	**Internet protocol**	Routing	**(Gateway)**	**IP address**

Gateway– the “post office”

A routing interface (not the whole router) for a LAN is called a gateway interface for that LAN. Different LAN has their own gateway interface, and it is accessible by its local computers, this means it has an interface that belongs to that local network.

Computers in the same LAN have the same network ID, in this case a switch can forward the traffic differently to the destination host.

However, computers in different networks have different network IDs.

When a packet goes to a remote destination (in a different network and the destination IP address has a different network ID), the switch simply forwards it to the gateway interface. In this case, the initial destination Mac address is the gateway’s address despite that the destination IP address is in a different network.

Internal components in a router

Hardware: e.g.

- CPU (central processing unit)
- RAM (random access memory)
- NVRAM (Nonvolatile random-access memory)
- Buses (internal data transmission channel between components of a computer)
- ROM (read-only memory)
- Interfaces
- Power

Firmware: e.g.

- Cisco's internetworking operating system IOS), IOS traditionally is seen as a monolithic operating system. Cisco also has specialised OSs such as NX-OX)
- Juniper's JunOS, seen as a modular operating system based on the FreeBSD kernel.
- VyOS : an open source operating system based on Debian Linux
- and DD-WRT*(also Linux based) etc.

Routing - IP packet forwarding

A router is able to connect two or multiple different networks

A router has a routing table (comparing to Mac-address table in switching's case)

A routing determines where it should forward traffic from a network to other network based on its routing table

Check routing table:

Show ip route

```
     61.0.0.0/25 is subnetted, 1 subnets
R       61.3.50.0 [120/1] via 172.16.100.2, 00:00:06, GigabitEthernet0/2
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.100.0/30 is directly connected, GigabitEthernet0/2
L       172.16.100.1/32 is directly connected, GigabitEthernet0/2
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/25 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
R1#
```

How to configure

“Tell the truth”

Interface gi0/1

Ip address 192.168.1.1 255.255.255.0 (I can see 192.168.1.0)

Interface gi0/2

Ip address 172.16.1.1 255.255.255.0 (I can see 172.16.1.0)

Router rip (routing protocol, we speak RIP language)

Version 2 (we speak contemporary language)

Network 192.168.1.0 (I can see 192.168.1.0)

Network 172.16.1.0 (I can see 172.16.1.0)

Steps of routing installation (General procedures)

- Analyse business requirements: identify needs of subnetworking, addressing, segmentation, topology etc.
- Review system design, refer to the version and timestamp, make sure is correct and ask for confirmation.
- Review and backup existing configuration, e.g. security parameters
- Develop basic parameters, e.g credential, Ip addressing, and protocols, zones, segmentations etc.
- Develop work plan, checklist, and performance benchmark
- Complete system testing and documentation
- Handover to clients and request sign-off

Steps of router configuration (Technical procedures)

- ❑Implement subnetworking, e.g. creating vlans
- ❑Implement ip interface and addressing, setting up gateways
- ❑Configure routing protocols and redistribution, including inter vlan routing
- ❑Configure access controls (ACL) and packet fliting
- ❑Configure other performance parameters, such as NAT
- ❑Secure the devices, develop access control list, authentication/passwords, ssh, encryption, and zoning

Ip route table

```
     61.0.0.0/25 is subnetted, 1 subnets
R       61.3.50.0 [120/1] via 172.16.100.2, 00:00:06, GigabitEthernet0/2
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.100.0/30 is directly connected, GigabitEthernet0/2
L       172.16.100.1/32 is directly connected, GigabitEthernet0/2
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/25 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
R1#
```

In above case 61.3.50.0 is a remote destination, although it is not connected to the router R1

R1 knows it can ultimately get to this destination via a local interface 172.16.100.2

The letter "R" means this route is learned though a protocol "RIP" from its neighbour

IP packet forwarding – principle

A router is able to connect two or multiple different networks

A router has a routing table (comparing to Mac-address table in switching's case)

A routing determines where it should forward traffic from a network to other network based on its routing table

Check routing table:

Show ip route

Ip route table

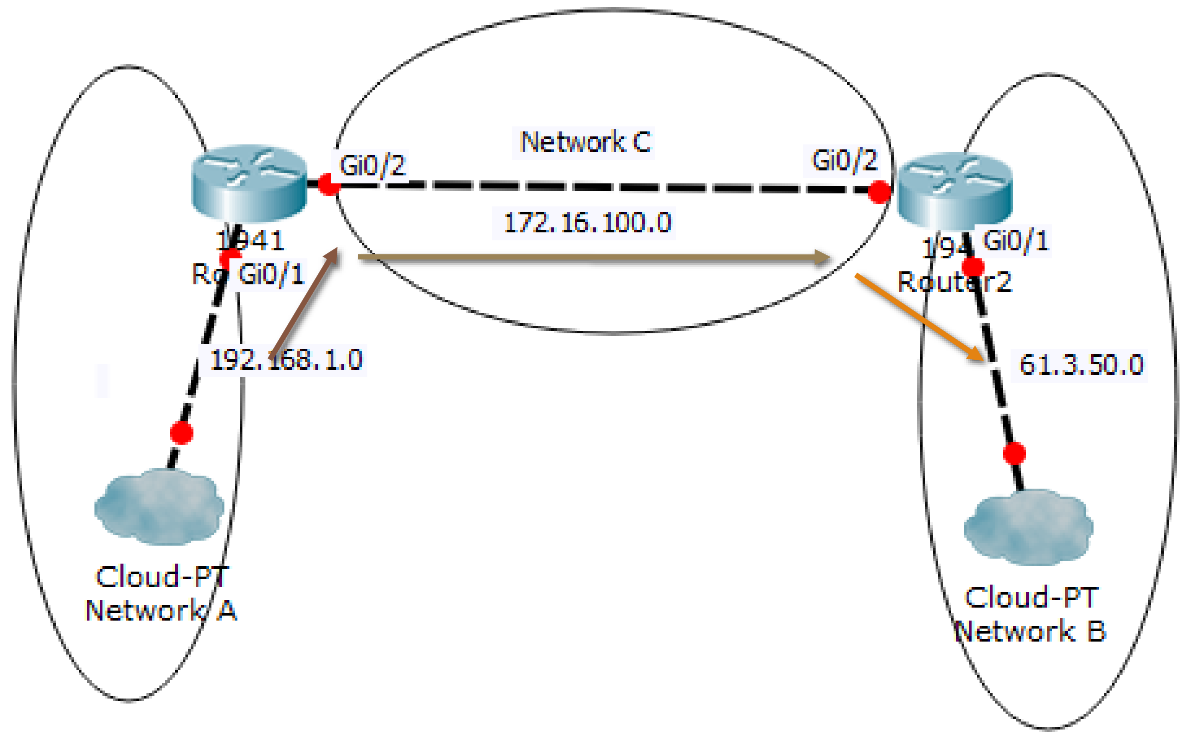
```
      61.0.0.0/25 is subnetted, 1 subnets
R        61.3.50.0 [120/1] via 172.16.100.2, 00:00:06, GigabitEthernet0/2
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.100.0/30 is directly connected, GigabitEthernet0/2
L        172.16.100.1/32 is directly connected, GigabitEthernet0/2
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/25 is directly connected, GigabitEthernet0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/1
R1#
```

In above case 61.3.50.0 is a remote destination, although it is not connected to the router R1

R1 knows it can ultimately get to this destination via a local interface 172.16.100.2

The letter "R" means this route is learned though a protocol "RIP" from its neighbour

```
     61.0.0.0/25 is subnetted, 1 subnets
R       61.3.50.0 [120/1] via 172.16.100.2, 00:00:06, GigabitEthernet0/2
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.100.0/30 is directly connected, GigabitEthernet0/2
L       172.16.100.1/32 is directly connected, GigabitEthernet0/2
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/25 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
R1#
```



“SYNTAX” OF STATIC ROUTING

Pseudocode :

- I am going to Place A through my neighbouring place B.
- I am going to any unknown places through my neighbouring place B.

Ip route static <u>A’s network ID</u> <u>B’s IP address</u> (next hop)

Ip route static <u>0.0.0.0 0.0.0.0</u> <u>B’s IP address</u> (next hop)

How routers learn the destinations and routes

R1 has two interfaces, the are connected to two networks

One of these two interfaces share the same network with another router (e.g. 172.16.100.0), this means these two routers can speak to each other directly, they are neighbours.

Neighbours tell each other the which networks are connected to them, so they know another router can help them to deliver packet to some more destinations that are not connoted to itself, e.g. 61.3.50.0

In summary

Each router just needs to tell the “truth” about what it can see.

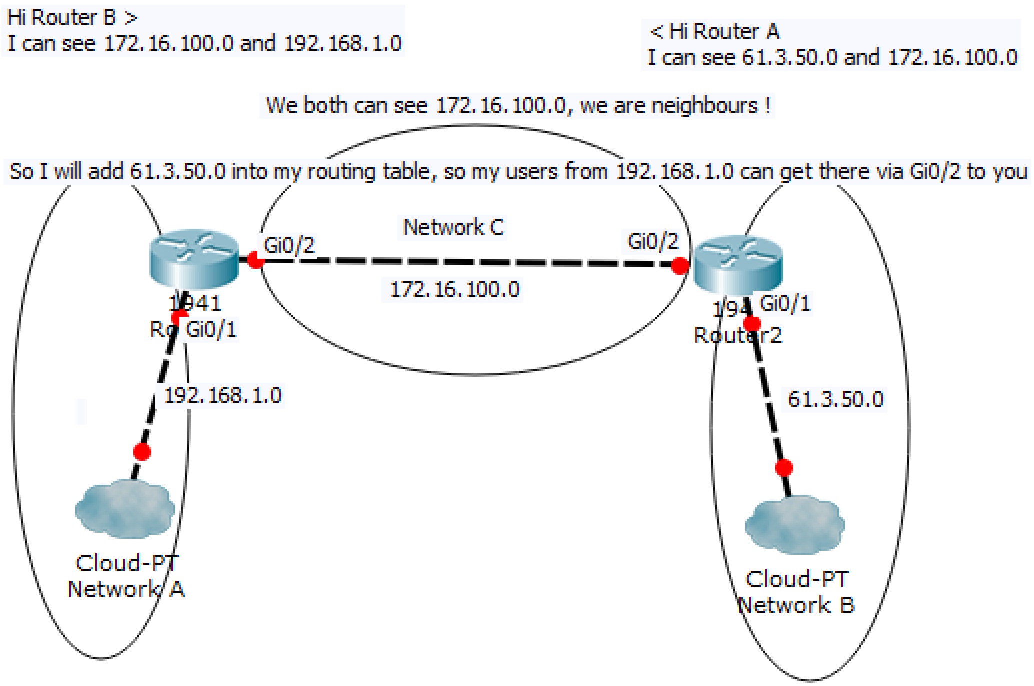
Other routers will determine if they are neighbours, if yes, they can help each other.

Therefore networks connected to Router B (61.3.50.0) can be reached by router A, so router A will copy router A’s links as its own reachable destinations.

Traffic from 192.168.1.0 on router A can get to 61.3.50.0 behind router B

How routers know which interfaces is point at which destination

Tell the “truth” and the neighbours will learn.



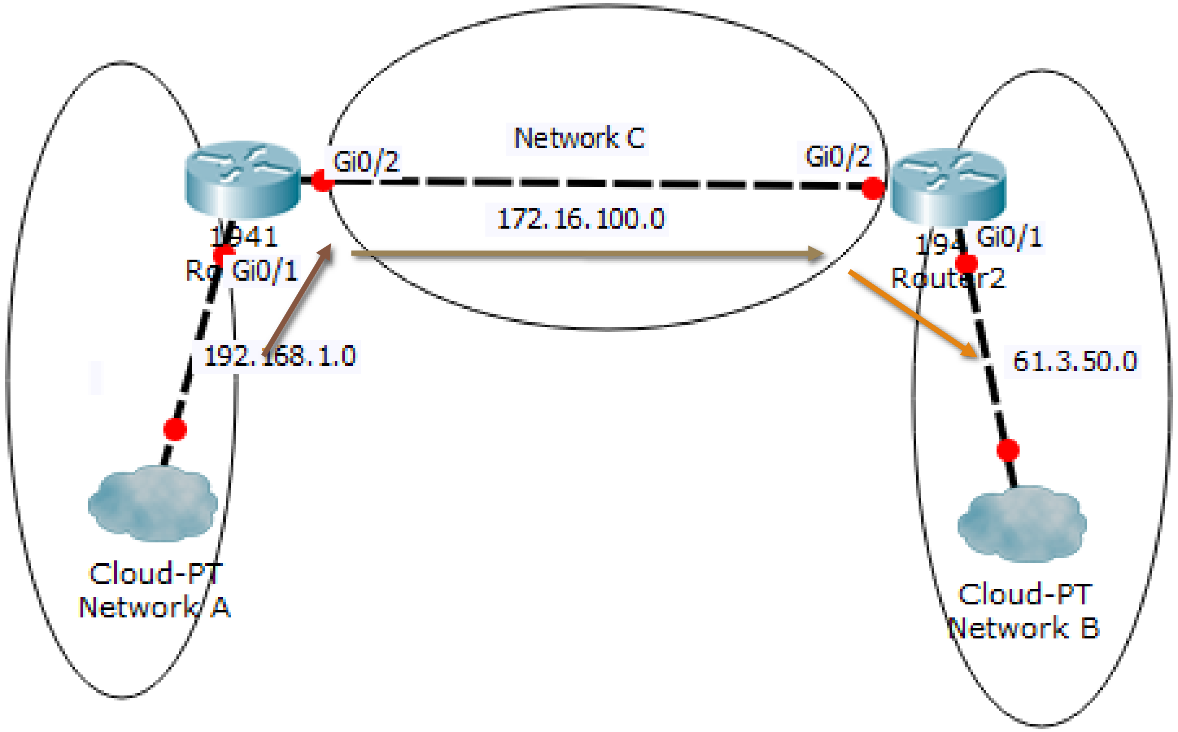
OSPF – Open shortest path, non-proprietary or use link-state, use process and areas, has different router roles, use cost as its metric

RIP – Routing information protocols, distance vector protocols, use hop counts as its metric

BGP – Boarder Gateway protocol. Exterior gateway protocol, path-vector routing protocol.

EIGRP – Enhanced interior gateway routing protocol, proprietary protocols, distance-vector protocols, only use incremental updates.

```
     61.0.0.0/25 is subnetted, 1 subnets
R       61.3.50.0 [120/1] via 172.16.100.2, 00:00:06, GigabitEthernet0/2
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.100.0/30 is directly connected, GigabitEthernet0/2
L       172.16.100.1/32 is directly connected, GigabitEthernet0/2
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/25 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
R1#
```



Another example: larger networks

Tell the truth:

Interface gi0/1

Ip address 192.168.1.1 255.255.255.0 (I can see 192.168.1.0)

Interface gi0/2

Ip address 172.16.1.1 255.255.255.252 (I can see 172.16.1.0)

Router eigrp 1 (routing protocol, we speak eigrp language, in group 1)

Network 192.168.1.0 0.0.0.255 (I can see 192.168.1.0, 255 of them)

Network 172.16.1.0 0.0.0.3 (I can see 172.16.1.0, 3 of them)

Of course you can also tell your router where to go

Ip route (distination) “via” interface or next hop

E.g. ip route 61.3.50.0 255.255.255.0 172.16.100.2 (on router B)

ip route 61.3.50.0 0.0.0.255 gi0/2

01

I believe I have entered the right commands but the system doesn’t recognise it, what’s wrong?

02

What is vlan, how to create vlans?

03

What is dynamic routing, what is static routing.

Discussion:

Switching/Intranetworking

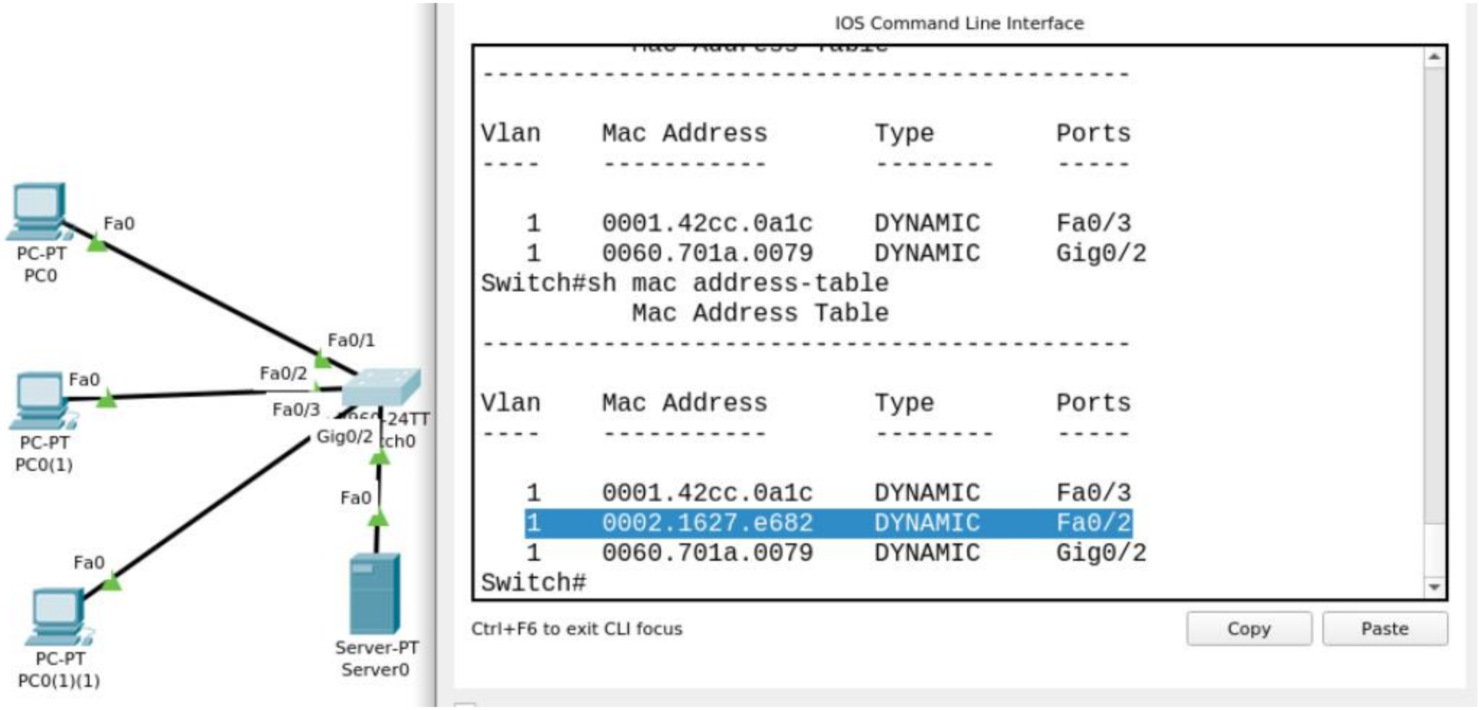
Learning outcomes

- How does a switch know where it should forward data to?
- How does a switch build and store its knowledge about the location of each hosts?
- What is IEEE802?

How do switches know each port and find each device

Once a switch receive a frame, it can check its source MAC addresses, and a record the port that this device is connected to.

Then the switch record both the port and the associated device's MAC addresses in a **Mac address table.**



Broadcasting domains and collision domains

Collisions may occurs when multiple devices send traffic at the same time on the shared network segment. A hub shares the same collision domain physically and doesn't not create new collision domain.

If devices can reach each other at the data link layer (OSI layer 2) by using broadcast, they form a broadcasting domain. This is typically a layer 2 network segment, it can be a physical LAN or a vLAN.

A switch port creates an independence collision domain.

The whole switch, by default is a broadcasting domain.

How to calculate domains:

A switch (L2) can separate collision domains, the number of switch ports may suggest the number of collision domains

A router can separate broadcasting domains, it works at layer 3 does not forward broadcasts. The number of router interfaces may suggest the number of broadcasting domains

Intra-networking

A local area network consists of computers that are geographically close to each other. Normally computers within the same LAN can reach each other without telecommunication circuits.

Logically, communication within a LAN is an intranetworking scenario. A switch can be used to form a LAN. A switch uses broadcasting to query new member computers and learns their MAC addresses.

Computers in the same LAN have the same network ID.

Local network (intranetwork)	IEEE 802.3	Switching /Mac address table	Broadcasting	Mac address

Switch

- Switches are Multiport Bridges.
- Switches provide a unique network segment on each port, thereby breaking collision domains.
- Today, network designers are replacing hubs in their wiring closets with switches to increase their network performance and bandwidth while protecting their existing wiring investments.
- Like bridges, switches learn MAC address information of data frames that are received from various computers on the network.
- Switches use this information to build forwarding tables to determine the destination of data being sent by one physical node to another physical node on the network.

01

How does a switch know where it should forward data to?

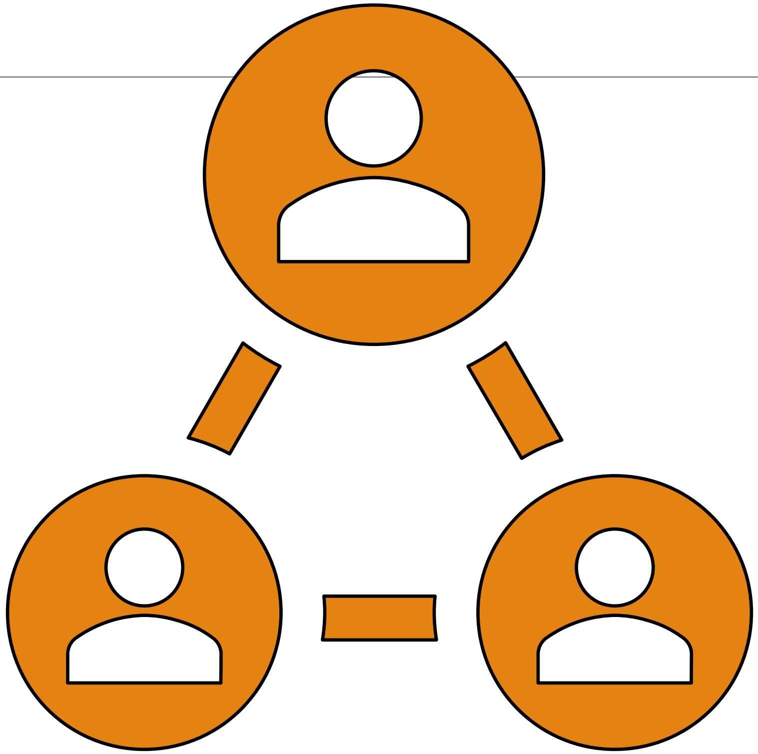
02

How does a switch build and store its knowledge about the location of each hosts?

03

What is IEEE802?

Discussion:



Basic Switching configuration

Mac-address Table

Show mac-address table

Show arp table

```
Sw1#sh mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0090.2bed.3c18    DYNAMIC     Fa0/24
Sw1#
```

Learning outcomes

- I believe I have entered the right commands but the system doesn't recognise it, what's wrong?
- What is vlan, how to create vlans?
- What is dynamic routing, what is static routing.

Vlan and vlan membership

Virtual Lan segment

Vlan 10

Name management

Interface fa0/10

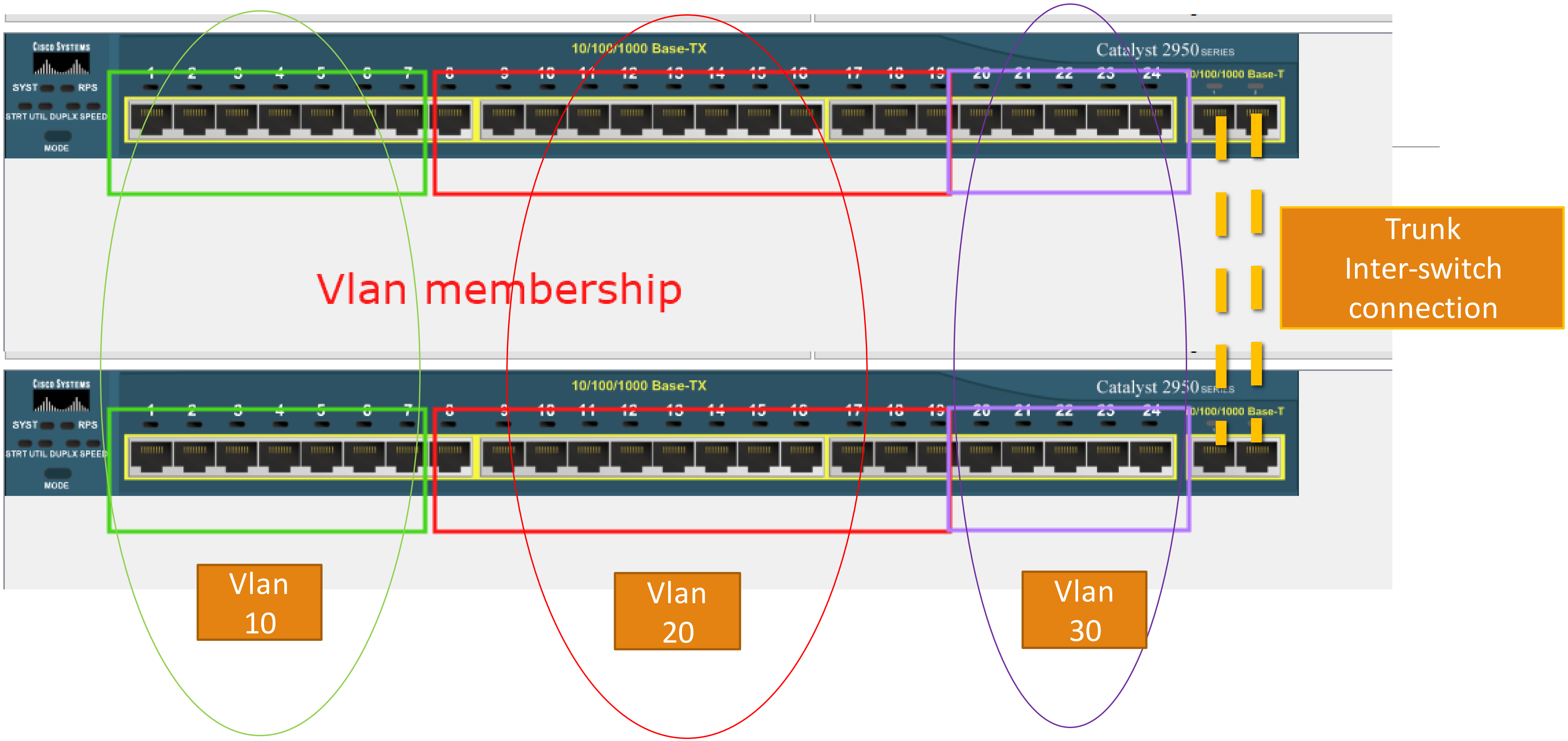
Switchport mode access

Switchport access vlan 10

VLAN is a logial network segmentation mechanism that helps separate network traffic with vlan membership for ports.

Vlan can be a reflection of organisational structure and functions.

Each vlan is a broadcasting domain.


10/100/1000 Base-TX
Catalyst 2950 SERIES
Vlan membership
Trunk Inter-switch connection
Vlan 10
Vlan 20
Vlan 30

Trunking (inter-switch connection)

Interface gi0/1

Switchport mode trunk

(or Switchport mode dynamic desirable)

Switchport trunk native vlan 1

VTP

Populate vlan configuration

Vtp mode server

(or vtp mode client)

Vtp domain DomainName

Vtp Passsword MyPassword

Switch ports

```
Sw1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4,
Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9,
Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13,
Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17,
Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21,
Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1,
Gig0/2
10   VLAN0010                         active
20   VLAN0020                         active    Fa0/5
```

They are layer 2 ports. They cannot have IP addresses.

Each of them is a collision domain

They have typically two modes: trunk or access

For access ports, they have to below to a particular vlan. If you don’t assign Vlan membership for them, they below to vlan 1 by default)

Vlan configuration

Vlan membership

Switch(config)# interface gigabitethernet0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 2

Summary

VLANS

Allows an administrator to logically group devices based on security requirements or business functions

Act as their a new network

Can be used to segment broadcast domains

Some benefits of VLANs include

Cost reduction,

Security,

Higher performance, management efficiency

Trunk

A trunk is a point-to-point link between one or more Ethernet switch interfaces and another networking device such as a router or a switch. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network.

Two trucking encapsulations are available on all Ethernet interfaces:

- Inter-Switch Link (ISL)—Cisco-proprietary
- IEEE 802.1Q— industry-standard

Trunking configuration

Switch(config)# interface gigabitethernet0/1

Switch(config-if)# switchport mode dynamic desirable

(or switchport mode dynamic auto)

Switch(config-if)# switchport trunk encapsulation dot1q

Switch(config-if)# switchport trunk allowed vlan 10

Summary

Trunks

A common conduit used by multiple VLANS for intra-VLAN communication

IEEE 802.1Q

The standard trucking protocol

Uses frame tagging to identify the VLAN to which a frame belongs

Does not tag native VLAN traffic

Trouble-shooting Vlan and trunking issues

Trunking mode mismatch

Native Vlan ID mismatch

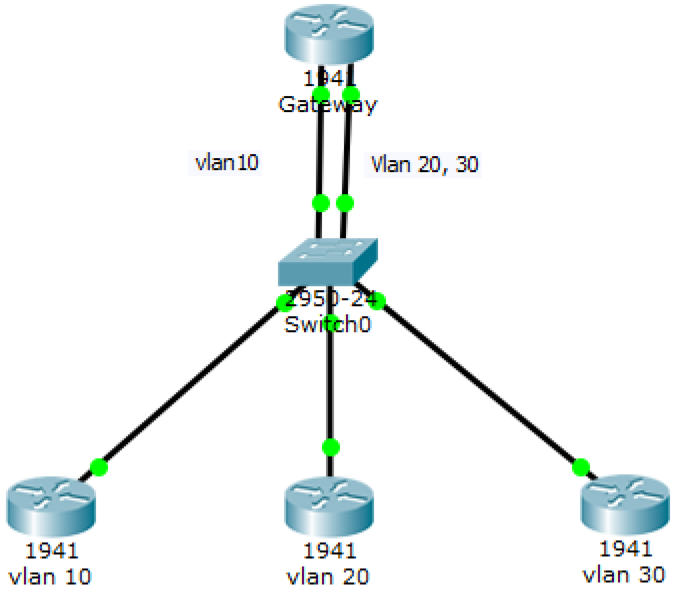
Vlan not allowed

Membership-network ID mismatch

Inter-vlan Routing

Configure Inter-VLAN Routing

Describe the steps to configure inter-VLAN routing



Inter-VLAN routing

Inter-VLAN routing is the process of routing information between VLANs

Inter-VLAN routing requires the use of a router or a layer 3 (or multiple-layer) switch

- open the layer 3 function on a switchports of a multilayer switch
- creating and use a virtual local area network (VLAN) interface

Traditional inter-VLAN routing

- Requires multiple router interfaces that are each connected to separate VLANs
- In this case, VLAN are treated as individual networks, each VLAN uses a router interface connected to the VLAN members as their gateway. All VLANs are advertised in routing protocols.

Option 1: Use routers for inter-vlan routing

The “internal” interface is access interface on the switch and another side is a routing interface, just like normal routing’s cases:

Switch(config)#interface fa0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

On the router’s side:

Router(config)#interface FastEthernet 0/1

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shutdown

And you need to configure routing, dynamic or static:

Router(config-router)# Router rip

Router(config-router)# Network 192.168.1.0

Router(config-router)# Network 200.200.200.0

Option 2: Use multi-layer switch for inter-vlan routing

The “internal” interface is a **vlan interface**:

Switch(config)#interface Vlan20

Switch(config-if)#ip address 192.168.2.1 255.255.255.0

Switch(config-if)#no shutdown

The external interface:

Switch(config)#interface FastEthernet 0/1

Switch(config-if)#no switchport

Switch(config-if)#ip address 200.1.1.1 255.255.255.0

Switch(config-if)#no shutdown

Routing table

200.200.200.0/30 is subnetted, 1 subnets

C 200.200.200.0 is directly connected, FastEthernet0/48

192.168.0.0/16 is subnetted, 3 subnets

C 192.168.1.0 is directly connected, Vlan10

C 192.168.2.0 is directly connected, Vlan20

C 192.168.3.0 is directly connected, Vlan30

S* 0.0.0.0/0 [1/0] via 200.200.200.2

Option 3: routing on-one-stick with subinterfaces

Int fa0/0

No ip address

No shutdown

Int fa0/0.1

Ip add 192.168.1.1 255.255.255.0

Int fa0/0.2

Ip add 192.168.2.1 255.255.255.0

https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html

Summary

Router on a stick

- this is an inter-VLAN routing topology that uses router sub interfaces connected to a layer 2 switch.
- Each Subinterface must be configured with:
- An IP address
- Associated VLAN number

Configuration of inter VLAN routing

– Configure switch ports connected to router with correct VLAN

– Configure each router subinterface with the correct IP address & VLAN ID

Verify configuration on switch and router

WAN and network scalability

WAN technologies

Circuit Switching

Creating a direct physical connection between sender and receiver, e.g. Dedicated leased T1/E1.

Message Switching

Each intermediary accepts the entire message, scrutinises the address, and then forwards the message to the next party,

Packet Switching All transmissions are broken into units called packets, these packets are then routed through various intermediaries, e.g. switched virtual circuits (SVCs) and permanent virtual circuits (PVCs).

X.25 is a packet-switching WAN technology

Frame relay, a simplified version of X.25 create virtual circuits (e.g. PVCs or SVCs) to connect remote LANs to a WAN. Frame is the PDU of frame-relay and it can be forwarded based on map.

Further reading:

http://docwiki.cisco.com/wiki/Introduction_to_WAN_Technologies

Fibre Distributed Data Interface. (FDDI)

FDDI token passing (Dual rings)

Internet (e.g. DSL, FTTX+LAN, 3G/4G, Satellite) + Virtual private network

MPLS Multi-protocol label switching, a technology routing technique in telecommunications networks that directs data from one node to the next based on short path labels. MPLS uses label-switched path (LSP).L3 MPLS VPN works with vrf (virtual routing and forwarding).

Note these protocols are not fully mapped to a single layer of OSI but mainly operate at one of these two layers.

WAN links

Cable modem.

Digital subscriber line (ADSL/VDSL).

Fiber-optic communication (e.g. nbn uses FTTX+LAN).

Leased line.

PSTN Dial-up.

Asynchronous transfer mode (ATM).

Mobile broadband (3G/4G/5G) has also become a WAN solutions.

VPN as WAN solutions

Ipsec VPN:

Confidentiality - > Encryption, e.g. DES, 3DES, ASE,

Authenticity ->Authentication Header

Integrity -> Digital Digest (Hash), e.g. MD5, SHA1

MPLS uses label-switched path (LSP)**.L3 MPLS VPN** works with vrf (virtual routing and forwarding).

WAN: Circuit Switching Vs Packet Switching

Switched circuits allow data connections that can be initiated when needed and terminated when communication is complete. This works much like a normal telephone line works for voice communication.

Packet switching is a WAN technology in which users share common carrier resources. Because this allows the carrier to make more efficient use of its infrastructure, the cost to the customer is generally much better than with point-to-point lines.

Continue

Some examples of packet-switching networks include Asynchronous Transfer Mode (ATM), Frame Relay, Switched Multimegabit Data Services (SMDS), and X.25.

A virtual circuit is a logical circuit created within a shared network between two network devices. Two types of virtual circuits exist: switched virtual circuits (SVCs) and permanent virtual circuits (PVCs).

X.25 and Frame-rely

X.25 - This is a set of protocols developed by the CCITT/ITU which specifies how to connect computer devices over an internetwork. These protocols use a great deal of error checking for use over unreliable telephone lines. They establish a virtual communication circuit.

Normally X.25 is used on packed switching PDNs (Public Data Networks).

Frame relay - uses frames of varying length and it operates at the data link layer of the OSI model. A permanent virtual circuit (PVC) is established between two points on the network

Frame relay does not store data and has less error checking than X.25.

Frame-relay commands

DLCI: Data link connection identifier.

Router(config)#interface serial 0/0/0

Router(config-if)#encapsulation frame-relay

Router(config-if)#interface serial 0/0/0.1 multipoint

Router(config-subif)#ip address 10.10.10.1 255.255.255.0

Router(config-subif)#frame-relay interface-dlci 102

Router(config-subif)#frame-relay interface-dlci 103

Router(config-subif)#interface serial 0/0/0.2 point-to-point

Router(config-subif)#ip address 10.10.20.1 255.255.255.0

Router(config-subif)#frame-relay interface-dlci 104

Frame-relay

Int s0/0

Encap frame-relay

Frame-realy lmi-type cisco

Frame-realy qos-autosense

Frame-realy **intf-type** [**dce** | **dte** |**nni**]

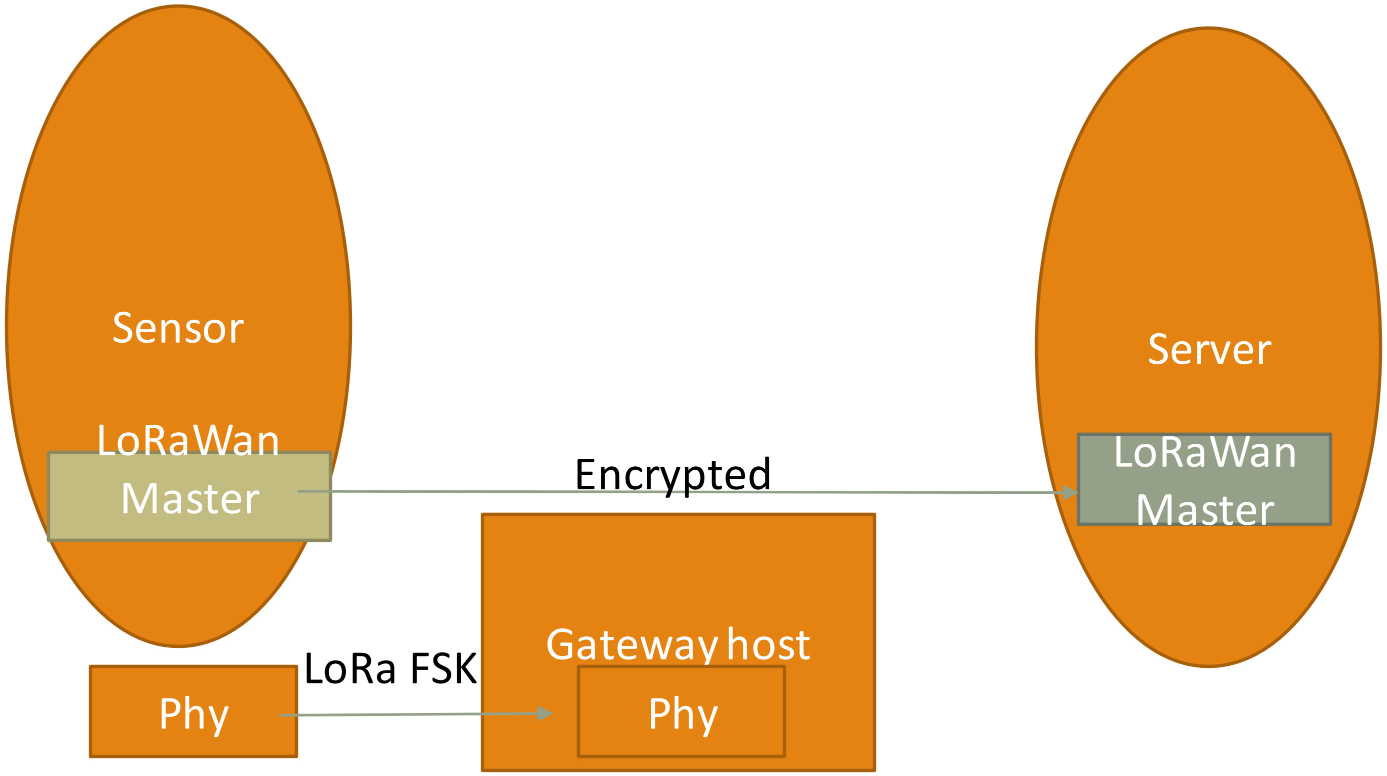
LoRaWAN

This is a long range point-to-multipoint networking protocol based on LoRa modulation scheme.

LoRaWAN uses a star topology with a gateway as the hub. It works at different frequency – in Australia it is 915MHz.

It is based on medium access control (MAC) layer protocol but it has the function similar to routing protocol working between the nodes and gateway.

Symphony Link , IEEE 802.11ah can be used as an alternative for LoRaWan.


Sensor
LoRaWan
Master
Encrypted
Server
LoRaWan
Master
LoRa FSK
Phy
Gateway host
Phy

Connection process for enterprise networks using WAN services and applications

- Consider the geographic distribution of users
- Applications that users need to access (e.g. VOIP, video conferencing, finance transaction, file transmission, etc.
- Performance requirements: bandwidth, latency, packet loss, up time.
- Consider installation cost and running cost
- Consider new technologies, e.g. MPLS VPN.
- Select the service provider.

Access control lists
Control access to network services and applications across the network

Steps to configure and activate access networks

Connect to local network node, e.g. a switch or ISP’s network

Enable TCP/IP stack and configure IP interfaces

Configure network addresses and gateway

Configure authentication (if necessary)

Configure access control

Standard and extended access list

Standard (ID normally from1 to 99)

access-list ID {permit/deny} {host/source source-wildcard/any}

E.g. access-list 10 permit 192.168.10.0 0.0.0.63

Int fa0/0

Ip access-group 10 in

Extended (ID from100 to199 or 2000 to2699):

access-list ID {permit/deny} {tcp/ip/icmp} {source: host/source source-wildcard/any} {destination: host/source source-wildcard/any} eq {protocol/port ID}

E.g. access-list 10 permit tcp192.168.10.0 0.0.0.63 host 200.200.200.1 eq www

Int fa0/0

Ip access-group 10 out

Standard vs Extended access control list

A standard ACL

- Only checks ACL source address
- Does not specify Layer 4 protocols and ports
- With ID 1-99, 1300-1999

An extended ACL

- Checks both source and destination address
- Specifies specific Source and destination protocols (IP, ICMP, UDP, TCP), application types (telnet, www), TCP and UDP ports
- With ID 100-199, 2000-2699

ACL examples

- IP address group 172.16.2.0/26 can access the internet except for telnet and ftp.

Think about the order :

Access-list 100 permit ip 172.16.2.0 0.0.0.63

Access-list 100 deny tcp 172.16.2.0 0.0.0.63 eq telnet

- IP address group 172.16.2.128/26 can access the web, but not ping and echo,

Access-list 100 deny icmp

IP address group 172.16.1.0/24 can access ssh and https only

- Internal server 172.16.100.1 can only be access by internal users.

These are internet users: 172.16.2.0/26, 172.16.2.128/26,172.16.1.0/24 so you need to have three statement in the same ACLs.

- The ISP requires the client's gateway drops any inbound traffic to XYZ's to be blocked if private IP address is identified from the ISP side.

1) What are Private IP addresses (three groups)?

- 192.168.0.0 0.0.255.255
- 172.16.0.0 0.15.255.255
- 10.0.0.0 0.255.255.255

2) In or out?

"Hidden" rules of applying access-list

One access list per interface, per protocol, and per direction

"Single match in a top-down order"

Implicitly deny by the system for unspecified traffics: deny ip any any

ACL lines can be added to numbered standard or numbered extended ACLs by sequence number

ACL “hidden rules”

First match is the only functional match

Orders matter – put more specific before more general ones

Implicit deny at the end

Access lists filter network traffic, it monitors and determines whether packets entering or leaving the interfaces of the network device should be forwarded or blocked.

There are :

IOS (or IP) access control list

Vlan Access control list

Port Access control list

IOS/IP access control lists

Access list criteria include:

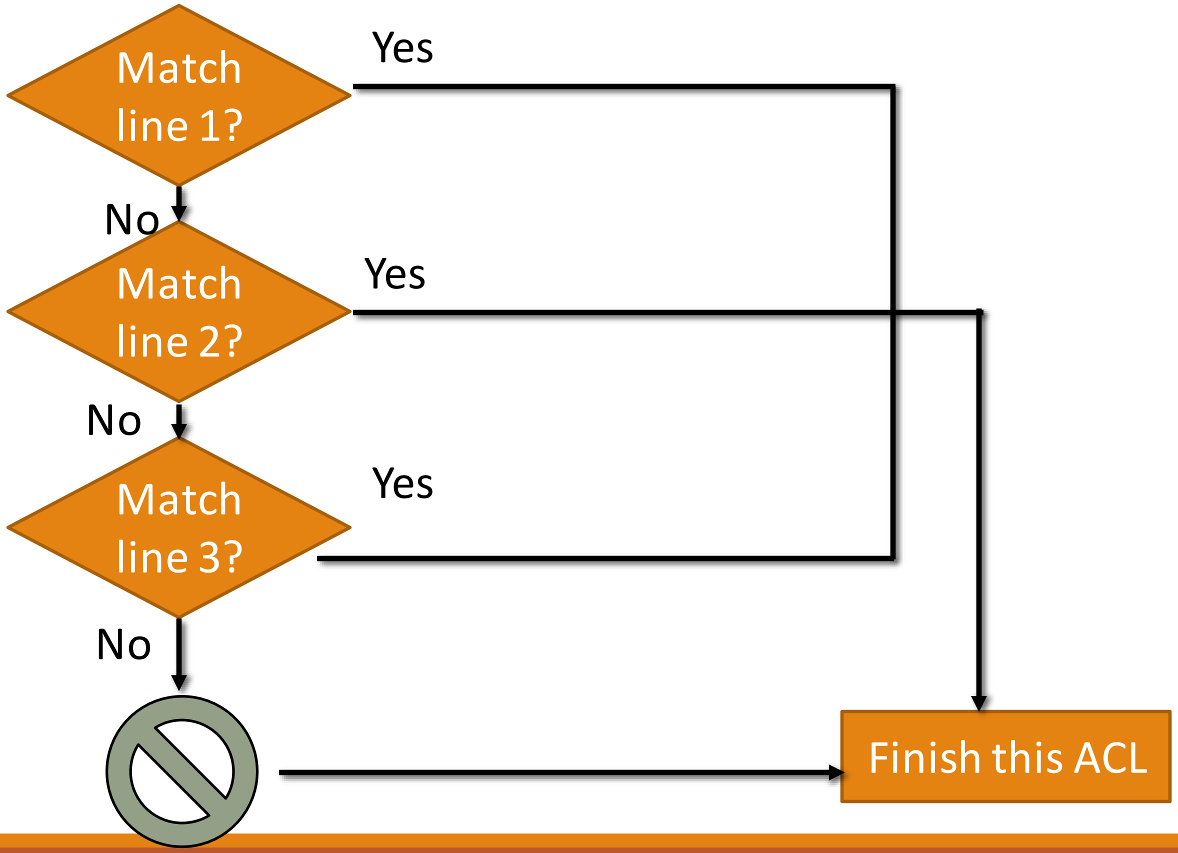
- the source address of the traffic,
- the destination address of the traffic,
- the upper-layer protocol,
- Other features (timer).

When to Configure Access Lists

used in "firewall" router between your internal network and an external or between two “zones” of your internal networks.

How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

Use a flow chart to show how ACLs operate



Syntax of ACL

access-list access-list-number {permit|deny} {host|source source-wildcard|any}

access-list access-list-number
[dynamic dynamic-name [timeout minutes]]
{deny|permit} protocol source source-wildcard destination destination-wildcard [precedence precedence]
[tos tos] [log|log-input] [time-range time-range-name]

Syntax of ACL

username *user-name* **password** *password*
interface <*interface***>**
ip access-group {*number|name***} {in|out}**

access-list access-list-number dynamic name {permit|deny} [protocol]
{source source-wildcard|any} {destination destination-wildcard|any}
[precedence precedence][tos tos][established] [log|log-input]
[operator destination-port|destination port]

line vty line_range

login local

How ACLs are Used to Secure an Enterprise Network and filter traffics.

The considerations for creating ACLs

Configure access lists for each network protocol configured , on the router interfaces.

inbound traffic or outbound traffic

Be careful about the order, only the first match works.

Take notes and do “what is” analysis.

There is always an implicit deny.

Learning activity

Prepare your configuration script based on the following network.

You need to design access control list to enable 192.168.1.0/24, 172.16.2.0/26, 172.16.2.128/26 to visit the external network

- Enable 172.16.2.0/26 to access web, ssh, and pop3
- Enable 172.162.2.128/26 to all services except for telnet.
- Enable 192.168.1.0 to web services only
- Block any other traffics

You need to design PAT to translate 192.168.1.0/24, 172.16.2.0/26, 172.16.2.128/26 to the interface

Implement your network and upload our journal.

ACL Rules and guidelines

Router IOS stops testing conditions after it encounters the first match. Therefore a packet, once matches an access control list, will either be dropped or forwarded and will not be matched by another access contro list.

An access list can control traffic arriving at a device or leaving a device, but not traffic originating at a device.

Only one access list per interface, per protocol, and per direction is allowed.

must contain at least one **permit** statement

An interface or command with an empty access list applied to it permits all traffic into the network.

Inbound access lists process packets before the packets are routed to an outbound interface. Outbound access lists process packets before they leave the device.

There is always a implicitly deny at the end.

After any statement by using the **remark** command.

ACL Configuration and trouble-shooting guidelines

ACLs, regardless their types, include the identifier (IDs of names), sequence, targeting traffic (IP address, mac address, pr otocols, directions), actions. Defining Criteria for Forwarding or Blocking Packets.

Use a model (e.g. flowchat to check ACLs)

1. **Check and match ID and names**
2. **Check scopes of the address (host, any, wildcards, the more specific the earlier)**
3. **Check other existing ACLs (be aware of other ACLs overriding the current one, especially "deny")**
4. **Check protocols, the lower the layer it works at the later**
5. **Check actions,**
6. **Check the order of statements**
7. **Check location of deployment and directions (**
8. **Be aware of implicit deny.**

Review : https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/12-4t/sec-data-acl-12-4t-book/sec-acl-ov-gdl.html

Network address translation (NAT)

Translate from private IP addresses into public ones so that packets can be routed on the public networks.

It also works for a large number of hosts in the stub domain communicate outside of the domain. NAT also hides the identity of hosts on the public network.

External local interface can be overloaded (shared) as Inside Global Addresses

It works with an access control list to specify the source

Static address translation/Dynamic address translation (dynamic NAT)/Overloading (PAT)

Access-list 10 permit 192.168.1.0 0.0.0.255

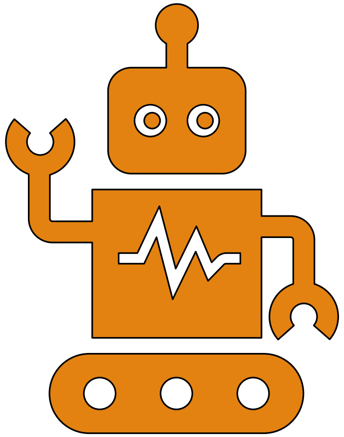
Ip nat inside source list 10 interface fa0/0 overload

Int fa0/0

 ip nat outside

Int fa1/1

 ip nat inside



Configure routing and switching with Command Line interface

01

Out of the “comfort zone”- What can you do with CLI in stead of GUI?

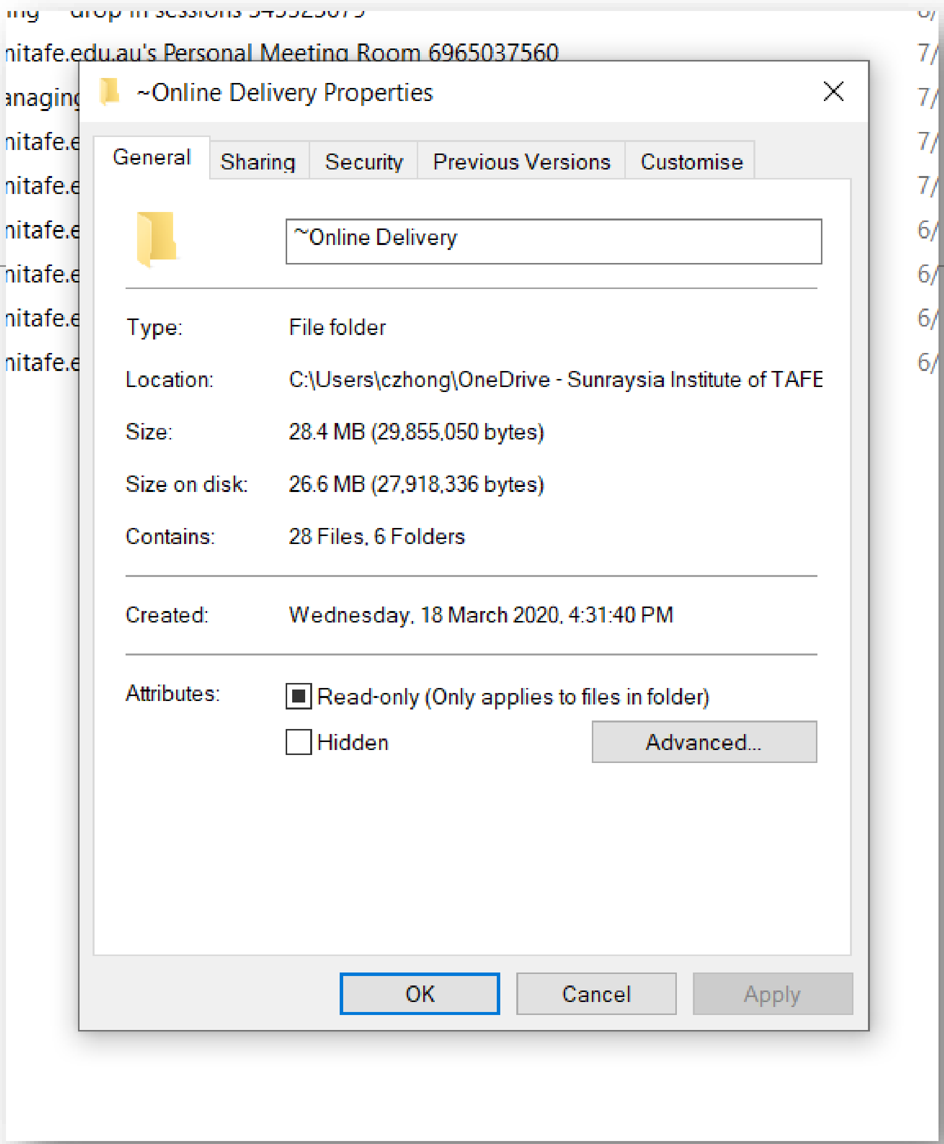
02

Learning configuration with the assistance of your devices. What is “interactive configuration? “

03

Under standard different modes.

Learning outcomes:


nitafe.edu.au's Personal Meeting Room 6965037560
~Online Delivery Properties
General
Sharing
Security
Previous Versions
Customise
~Online Delivery
Type:
File folder
Location:
C:\Users\czhong\OneDrive - Sunraysia Institute of TAFE
Size:
28.4 MB (29,855,050 bytes)
Size on disk:
26.6 MB (27,918,336 bytes)
Contains:
28 Files, 6 Folders
Created:
Wednesday, 18 March 2020, 4:31:40 PM
Attributes:
Read-only (Only applies to files in folder)
Hidden
Advanced...
OK
Cancel
Apply

IOS CLI Hierarchy

Commend line interface normally arrange commends based on a hierarchy of naming convention of network elements. Normally a command contains action words and operation parameters.

- Global configuration mode
- Interface configuration mode
- Router configuration mode
- Line configuration mode
- Debbug mode

Interactive configuration

Using pre-built prompts to verify and assist your configuration

“?” and “Tab” key

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15mt/fundamentals-15-mt-book/cf-cli-basics.pdf

Searching and Filtering CLI Output Examples with “pipe”.

Initial (basic) configuration

Look at Resource : http://and discuss:

www.cisco.com/c/en/us/td/docs/routers/access/1900/software/configuration/guide/Software_Configuration/routconf.html#15062

configure terminal

hostname name

enable secret password

no ip domain-lookup

And ssh/telnet,

log,

authentication,

ntp,

I/O memory allocation

Banner

Vlan interface

The debates on CLI vs GUI.

- Better Control.
- Speed and efficiency.
- Flexibility
- Ease access
- Support batch processing,
- Support programming and automation
- Very interactive
- Informative, real time, comprehensive status reports.

Preparation for configuration

Overview

1. Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts

2. Perform, save and verify initial switch configuration tasks

3. Implement and verify ***basic security for a switch***

User EXEC

2. Perform, save and verify initial switch configuration tasks

As a security feature, Cisco IOS software separated the EXEC sessions into two access levels:

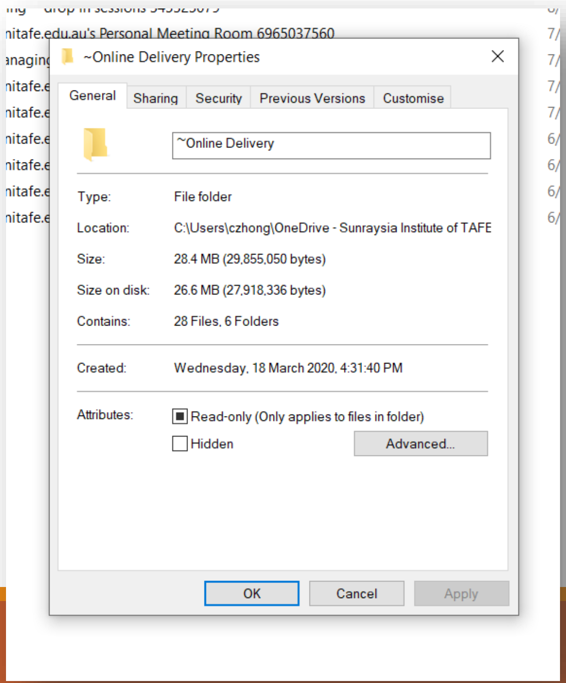
User EXEC: limited number of basic monitoring commands, default mode , identified by the > prompt.

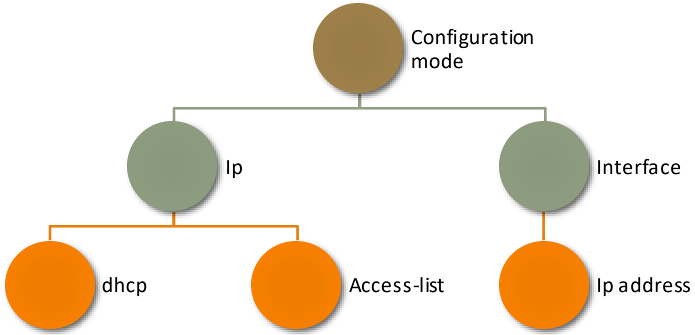
Privileged EXEC: access the switch for all device commands, can be password-protected, identified by the # prompt.

Configuration Modes

Cisco IOS software uses a hierarchy of commands in its command-mode structure (Refer tutorials).

Each command mode supports specific Cisco IOS commands related to a type of operation on the device.





Privileged EXEC

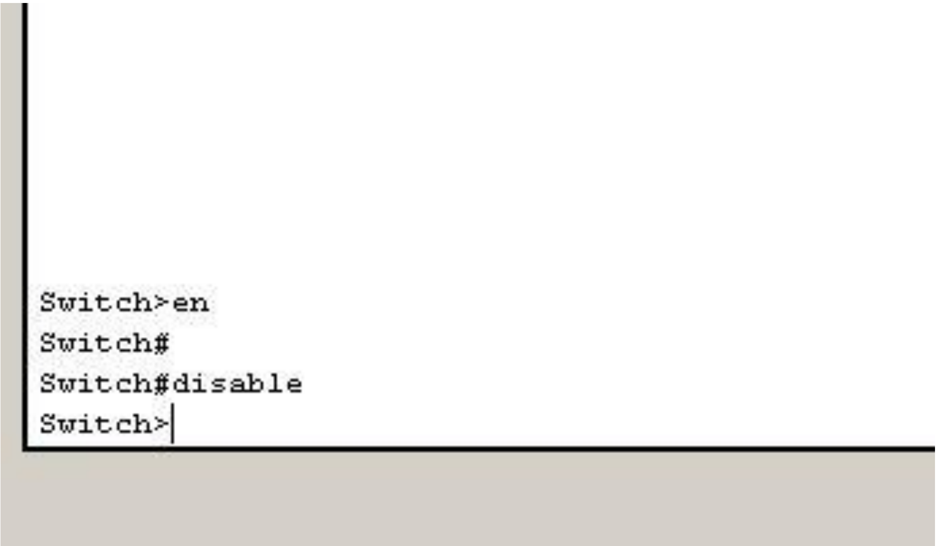
Enter the “enable” command (or “en” in short)

By default, the password is not configured.

Compare the following two commands:

Enable secrete PASSWORD

Enable password PASSWORD



Configuration Modes

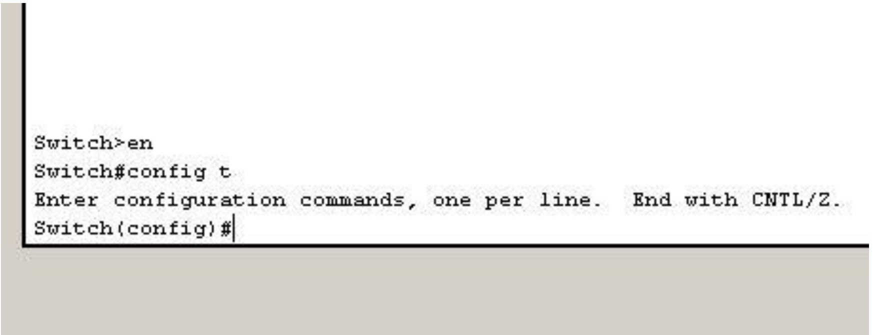
Global Configuration Mode:

To configure global switch parameters e.g.

the switch hostname or the switch IP address used for switch management purposes.

To access global configuration mode,

enter the “configure terminal” command in privileged EXEC mode. The prompt changes to (config)#.



Interface Configuration Mode

From global configuration mode, enter the “interface<interface name>” command. The prompt changes to (config-if)#.

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int F0/1
Switch(config-if)#
```

Using the help facility

The Cisco IOS CLI offers two types of help:

Help: enter the character sequence followed by a question mark (?). No space before the question mark.

A list of all available commands in the current context is displayed.

Enable telnet or secure vty ports with ssh

The vty ports on a Cisco switch allow you to access the device remotely.

it is very important to secure the vty ports.

To secure the vty ports from unauthorized access, you can set a vty password that is required before access is granted.

Crypto generate key rsa

ip ssh version 2

Line vty 0 4

Transport input ssh

Configure EXEC mode passwords

Privileged EXEC mode allows any user enabling that mode on a Cisco switch to configure any option available on the switch.

```
Switch(config)#enable secret cisco 123
Switch(config)#
```

You can assign an encrypted form of the enable password

```
Switch>enable
Password:
Switch#
```

01

In GUI you click tabs, and enter data into blanks,

What can you do with CLI?

02

I don’t know how to configure, what can I do? What is “interactive configuration? “

03

What are modes?

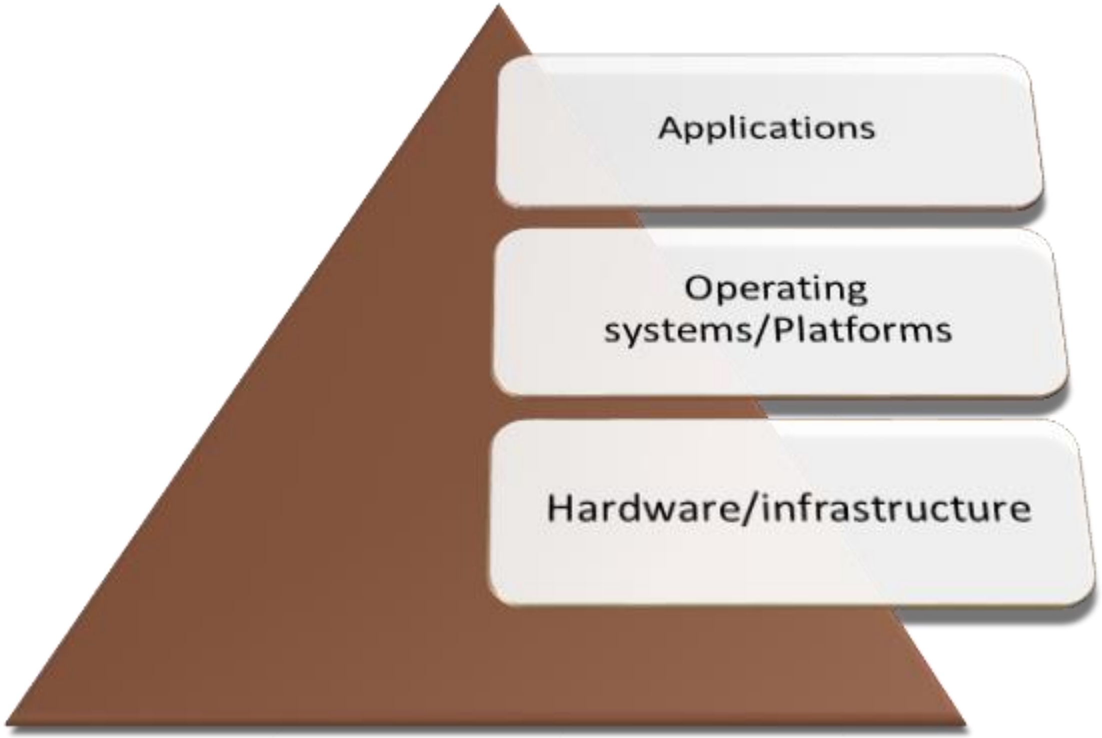
Discussion:

3. Network trouble-shooting - switches and routers

3.1 Monitor network performance and isolate faults using diagnostic and analysis tools

3.2 Troubleshoot network and internet connectivity according to manufacturer’s specifications and enterprise procedures

System Architecture



Configure, verify and troubleshoot routing protocols

- Analysis network segmentation and review existing configuration.
- Design addressing scheme,
- Determine protocols
- Define protocol parameters (e.g. areas, process IDs, autonomy system),
- Emulate existing network and test the interoperability of configuration.
- Debug and document configuration.
- Establish baselines
- Check misteach with given segmentation (unit test) and check connection from end to end (integration test).
- Using substation or other strategies to fix any issues identified.

Trouble shooting strategies

- Symptoms
- Segment
- Locations
- Hypothesis
- Test hypothesis
- Implement solutions
- Test solution

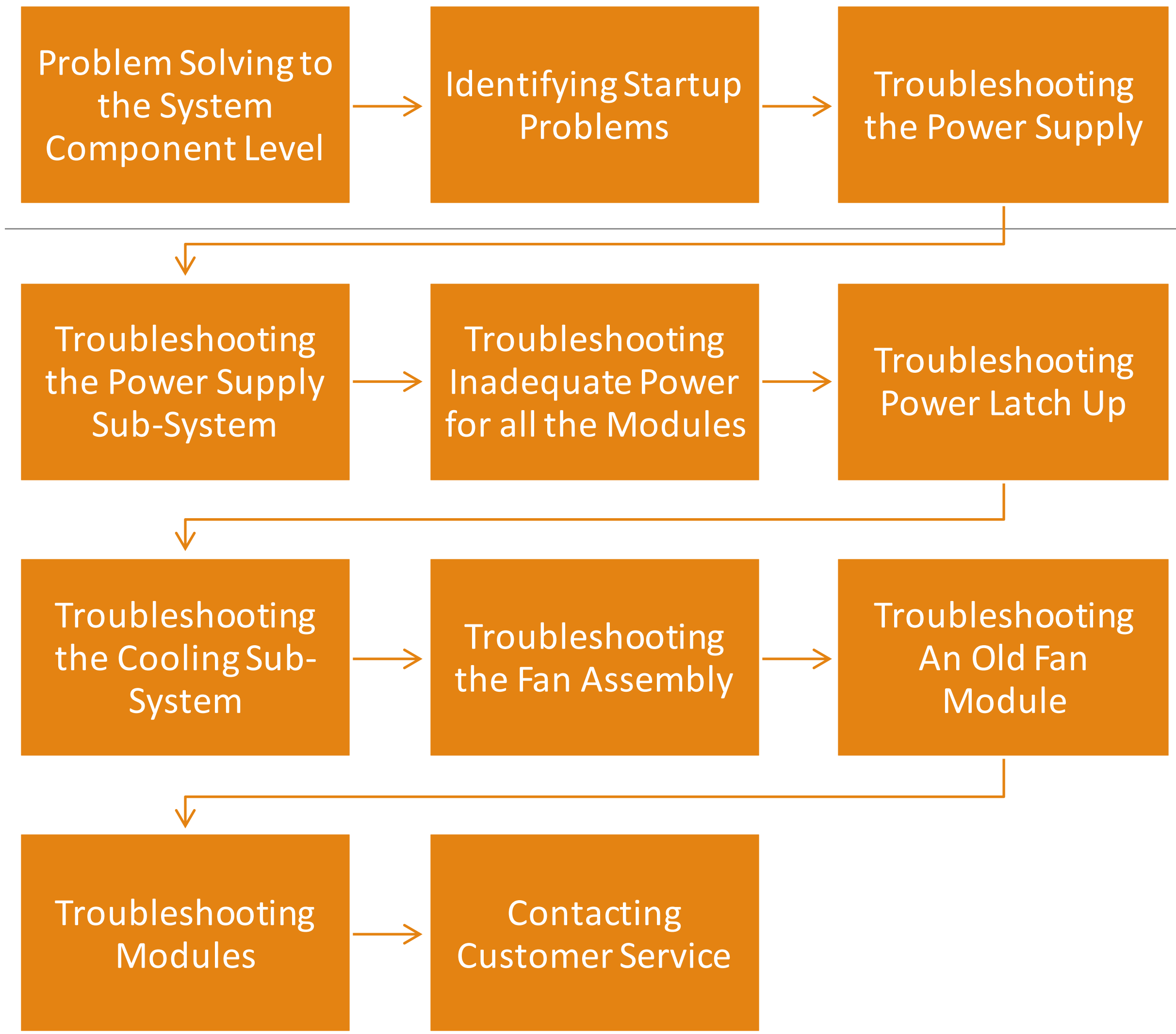
Identify	Identify the problem : identify an issue; e.g. the computer won't turn on.
Segment	Segment the system: map and split the system structure as different components.
Locate	Locate the problems within a certain segment.
Establish	Establish a theory of probable cause (assumptions) e.g. could be that the computer is not plugged in to the AC outlet.
Test	Test the theory to determine the cause : To test the theory, you would plug the computer in. if it doesn't work, you would go back and establish a new theory.
Establish	Establish a plan of action to resolve the problem and implement the solution : establish the plan of action based on that theory, and then implement your solution.

Verify full system functionality and, if applicable,

Implement preventative measures test and verify that the system is functioning correctly. Consider the risk of testing and have a backup plan.

Document findings, actions, and outcomes :

you want to document your findings and the outcome. In many companies, documentation begins right when you first get a troubleshooting call (or trouble ticket), and the documentation continues throughout the entire process. Be sure to keep track of what happened, why it happened, and how you fixed the problem.



Trouble shooting – checklist

Layer based trouble shooting

Layer	Possible issues	System unitalities
Layer 7	Authentication, traffic filting etc	Dependence on issues, check firewall and log, et.c
Layer 3	IP address mismatch, routing protocol mismatch, protocol parameter mismatch, access control misconfiguration, NAT mismatch	Ping, trace route, show ip interface brief,
Layer 2	Speed mismatch, duplex mismatch, vlan membership mismatch, trunking mismatch, port type mismatch, port security,	show interface, show interface trunk, show vlan
Layer 1	cable adapter mismatch, cable disconnected	Cable testing tools, e.g. Fluke.

Summary of fault-finding methods

Model based – use a logic **structure**, frameworks, or a set of benchmark **to** identify the issues.

Knowledge database – base on **abnormal cases** and some standard steps/guidelines (e.g. troubleshooting guidelines in the user manual of a products)

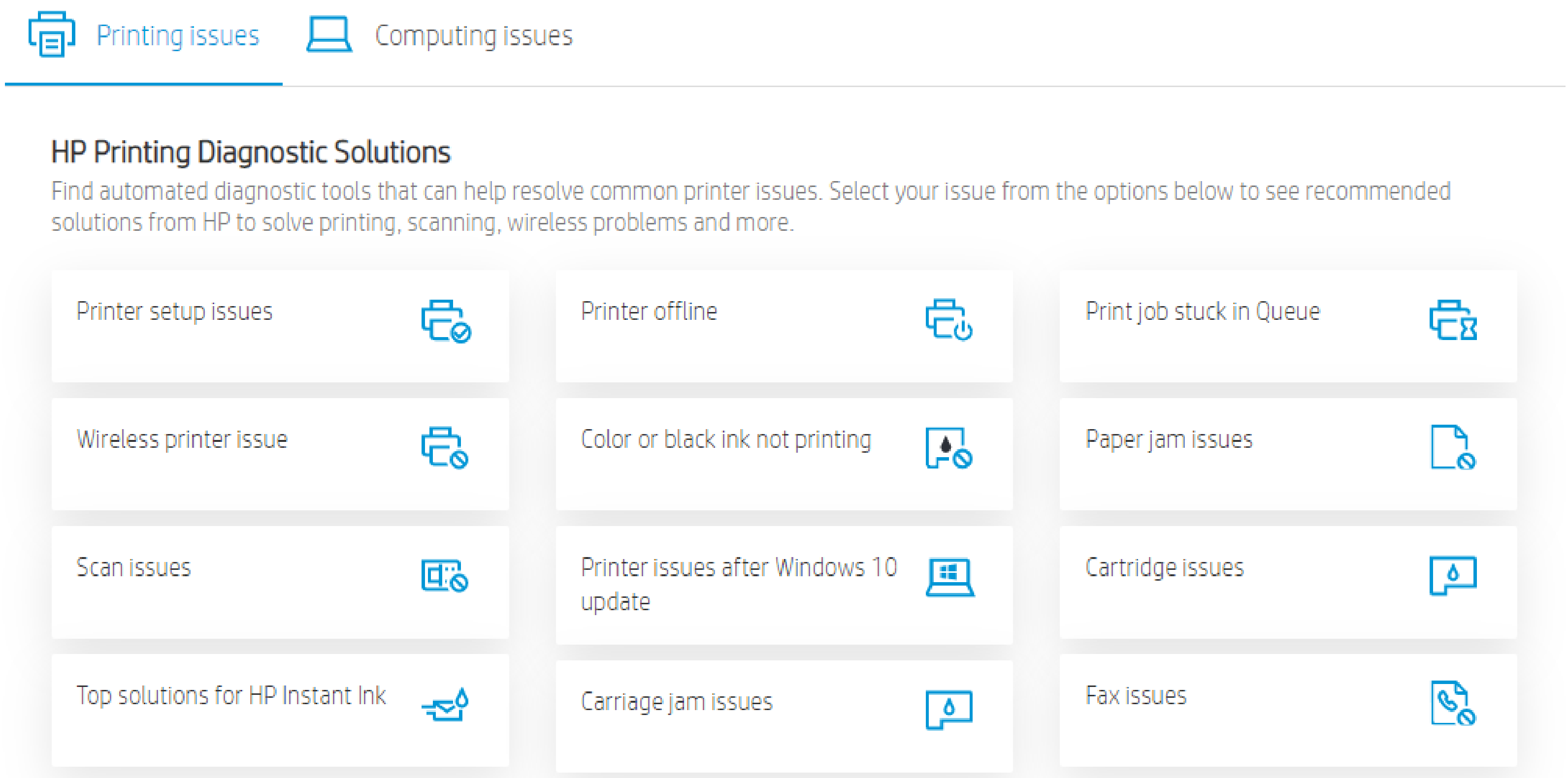
Debugging – observe the dynamic process of the system,

Substitution – replace some part or components to see the results

Simulation – rebuild a system of the same function and see the difference.

Knowledge database

Sometimes it is also called a case/solution library



Source: https://support.hp.com/us-en/topic/diagnostics Screenshot taken 03/08/2020

Solution and make provision for rollback

Problems	Variables to be tested	Possible causes	Rollback solutions
Two neighbouring routers don’t ping	Ip addresses, subnet masks, interface parameters	IP address mismatch, encaptualisation	Reconfigure Ip address and encaptualisation
PC can not get to other network	Gateway ip address,	Gateway misconfigured	Change gateway address
Missing routes	Routing issues, protocols, versions, autonomous system ID	IP misconfiguration, protocol mismatch, parameter mismatch	Network advsertisement

Solution and make provision for rollback

Problems	Variables to be tested	Possible causes	Rollback solutions
User PC cannot get to the internet	1 user PC's gateway configuration 2 gateway's routing table and routes verification" Show ip route" or "show ip interface"	User PC dose not set up gateway address. Gateway router does not have a the valid route due to current network not advertised	Add or remove Network advsertisement

Summary of fault finding methods

Function testing:

Unit testing.

Integration testing.

System testing.

Acceptance testing.

Performance testing

Load testing

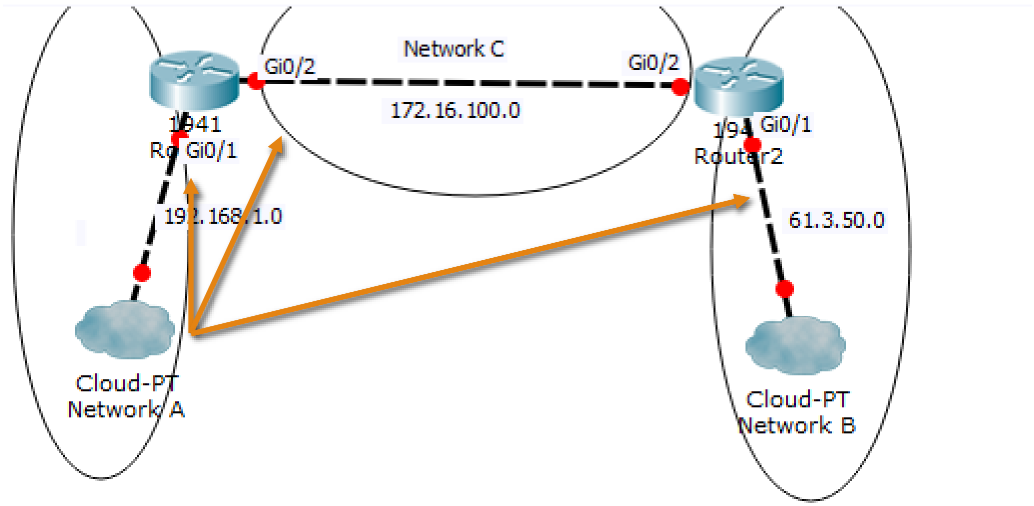
Compatibility testing

Security testing

Reliability testing

Example: how routers know which interfaces is point at which destination

Tell the "truth" and the neighbours will learn.



Example: how routers know which interfaces is point at which destination

Ping the gateway

Testing local network

Ping From the gateway to the ISP (or next hop)

Testing local routing

Ping from ISP to the destination

Testing backbone routing

Networking Data analysis - debug

```
IP-EIGRP neighbors for process 1
H   Address  Interface Hold Uptime   SRTT   RTO  Q  Seq
                   (sec)        (ms)       Cnt Num
3   192.168.1.1  Fa0/0    12  00:00:42    1  5000  1  0
2   198.168.1.3  Fa0/0    12  02:47:13   22   200  0  339
1   192.168.2.4  Fa1/0    12  02:47:16   24   200  0  318
0   198.168.2.3  Fa/0    12  02:47:13   20   200  0  338 13   20   200  0  338
```

Determine Hardware Symptoms – an example

Symptom: LED lights do not glow, display is black, computer does not start.

If there is no power available to the connections inside the computer, the LEDs will not glow, there will be no fan noises, and the computer will not startup. There are several things you can do to verify that power is available to the computer.

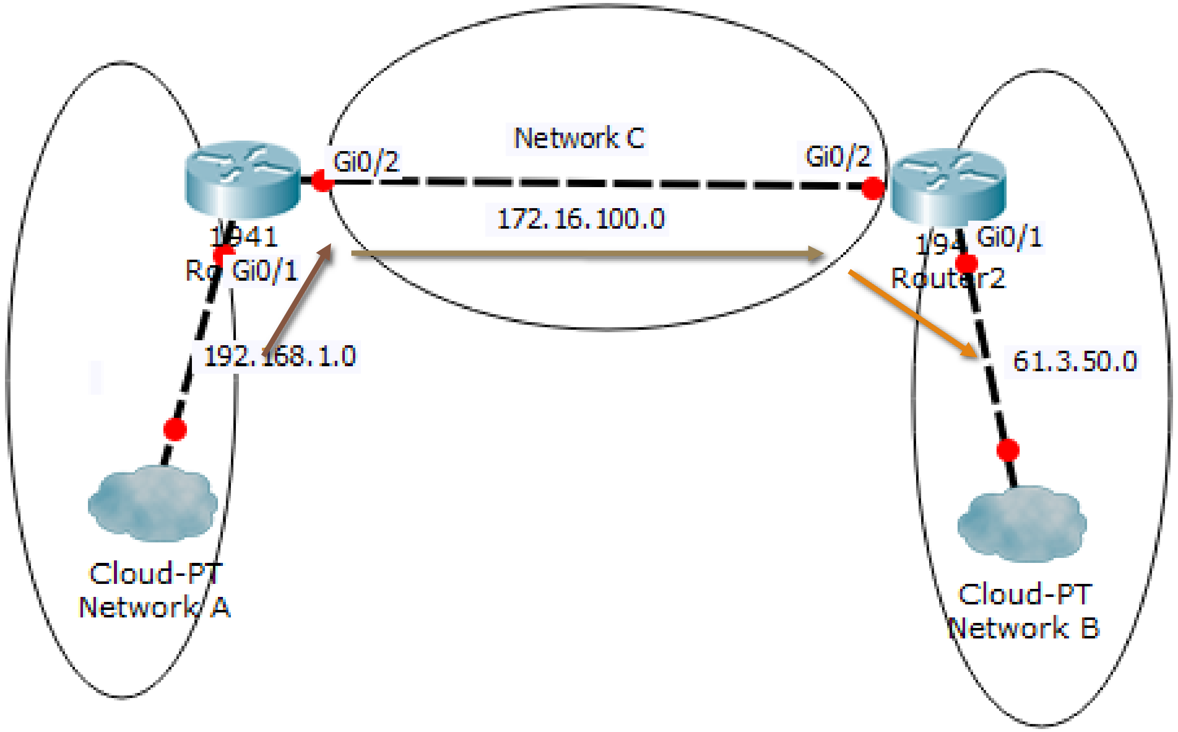
Hardware

- Check the condition of cables, components, and peripherals.
- Clean components in order to reduce the likelihood of overheating.
- Repair or replace any components that show signs of abuse or excess wear.
- Use the tasks listed in the figure as a guide to create a hardware maintenance program.

Hardware

- Check log, user manual, and organisational policies
- Set up safety signs and protections, request site access
- Check the condition of cables, components, and peripherals.
- Clean components in order to reduce the likelihood of overheating.
- Upgrade firmware if necessary.
- Repair or replace any components that show signs of abuse or excess wear.
- Check usage and replace consumables.
- Use the tasks listed in the figure as a guide to create a hardware maintenance program.
- Update maintenance log

```
      61.0.0.0/25 is subnetted, 1 subnets
R        61.3.50.0 [120/1] via 172.16.100.2, 00:00:06, GigabitEthernet0/2
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.100.0/30 is directly connected, GigabitEthernet0/2
L        172.16.100.1/32 is directly connected, GigabitEthernet0/2
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/25 is directly connected, GigabitEthernet0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/1
R1#
```



How to configure/misconfigure

Tell the truth:

Interface gi0/1

Ip address 192.168.1.1 255.255.255.0 (I can see 192.168.1.0)

Interface gi0/2

Ip address 172.16.1.1 255.255.255.0 (I can see 172.16.1.0)

Router rip (routing protocol, we speak RIP language)

Version 2 (we speak contemporary language)

Network 192.168.1.0 (I can see 192.168.1.0)

Network 172.16.1.0 (I can see 172.16.1.0)

How to configure/misconfigure

Tell the truth:

Interface gi0/1

Ip address 192.168.1.1 255.255.255.0 (I can see 192.168.1.0)

Interface gi0/2

Ip address 172.16.1.1 255.255.255.252 (I can see 172.16.1.0)

Router eigrp 1 (routing protocol, we speak eigrp language, in group 1)

Network 192.168.1.0 0.0.0.255 (I can see 192.168.1.0, 255 of them)

Network 172.16.1.0 0.0.0.3 (I can see 172.16.1.0, 3 of them)

How to configure/misconfigure

Tell the truth:

Interface gi0/1

Ip address 192.168.1.1 255.255.255.0 (I can see 192.168.1.0)

Interface gi0/2

Ip address 172.16.1.1 255.255.255.252 (I can see 172.16.1.0)

Router ospf 1 (routing protocol, we speak ospf language, in group 1 area 0)

Network 192.168.1.0 0.0.0.255 area 0 (I can see 192.168.1.0, 255 of them)

Network 172.16.1.0 0.0.0.3 area 0 (I can see 172.16.1.0, 3 of them)

How to configure/misconfigure

Ip route (remote destination) "via" interface or next hop

E.g. ip route 61.3.50.0 255.255.255.252 172.16.100.2 (on router B)

or

ip route 61.3.50.0 255.255.255.252 gi0/2

Note: Pointing at a local network is not a syntax issue but no valid route will be built in such a case.

Text analysis

Router 1	Router 2	Router 3
interface GigabitEthernet0/0 ip address 172.16.1.1 255.255.255.128 interface GigabitEthernet0/1 ip address 172.16.2.1 255.255.255.252 # (no issue found) router rip version 1 network 192.16.2.0 network 172.16.1.0 no -summaryip classless end	interface GigabitEthernet0/0 ip address 172.16.1.129 255.255.255.128 #(comparing to the diagram) interface GigabitEthernet0/1 ip address 172.16.2.2 255.255.255.252 # (no issue found) router eigrp 1 redistribute rip metric 1000000 1 255 1 1500 network 172.16.2.4 0.0.0.3 network 172.16.1.128 0.0.0.127 router rip version 2 redistribute eigrp 1 metric 1 network 172.16.1.0	interface GigabitEthernet0/0 ip address 172.16.0.1 255.255.255.0 interface GigabitEthernet0/1 ip address 61.122.12.1 255.255.255.252 duplex half interface GigabitEthernet0/2 ip address 172.16.2.6 255.255.255.252 router eigrp 11 redistribute static metric 1000000 1 255 1 1500 network 172.16.0.0 network 172.16.2.4 0.0.0.3 ip route 61.122.12.0 255.255.255.0 GigabitEthernet0/1

Commonly used tools – networking

- Ping
- Tracert
- NetStat
- NSLookup
- Wireshark

And

- Show ip interface brief
- Show interface
- Show ip access-list
- Show ip route

Commonly used tools- networking

Native tools embedded in the system, for example in router’s case:

Which categories - “ Ip, subnet masks”

- Show ip interface brief
- Show interface
- Show ip access-list
- Show ip route
- Ping

- Debug ip packet
- Debug ip eigrp

Summary of “Troubles” - Networking Protocols

- 1. Protocol mismatch(Trunking vs access, RIP vs EIGRP, version 1 vs 2)
- 2. Perimeter mismatch (Autonomous system ID, process ID and area ID etc. redistribution metrics)
- 3. Address mismatch (192.168.10.1 vs 172.168.10.1 vs. 172.16.10.1)
- 4. Adapter mismatch (serial, and ethernet)

A (knowledge) Database of problems/recommendation or solutions (1)

Symptoms	Information	Possible causes	Trouble-shooting tools	Solutions	Rollback	Testing	Prevention

A (knowledge) Database of problems/recommendation or solutions (2)

Problem ID	Symptom	Area	Category	Possible Causes	Severity	Solutions	Responsible person

Categories of testing methods

Faction testing:

- Unit testing.
- Integration testing.
- System testing.
- Acceptance testing.

Performance testing

- Load testing
- Compatibility testing
- Security testing
- Reliability testing

Summary of Trouble-shooting steps

Issue	Problems and requests recorded in a helpdesk ticket from the company's helpdesk system	Examples
Data collection	What data needs to be collected to identify the problem?	Models of hardware, version of driver or software, error code/types, indicators/ singalong. Configuration parameters, variables, using system tools and debugs,
Data analysis	What can you find from the data and information?	Interpreting codes/signals, compare protocols, parameters, variables, versions, debug
Symptoms	What are the symptoms?	Any issues that is not as designed. No connection, no signal, unexpected results, poor resolutions/performance, delay
Potential solutions	List potential solutions and justify the most appropriate solution?	Tunning, adjustment, replacement, upgrade, patching,
Tools	How do you obtain suitable tools and equipment to fix the problem (provide screenshots)?	System tools and debugs, third party testing tools,
Rollback	If the solution does not work, how will you rollback?	Backup and restore, command reversion
Verification	How do you test each step of the solution until you fix the problems?	Repeat step 1-2
Causes	What are the possible causes of the problem?	Parameter mismatch, addressing mismatch, protocol mismatch, adaptor mismatch, signal mismatch, power supply, disconnection, consumables, faulty hardware.
Trouble-shooting methods	What do you do to isolate and fix the final causes?	Model based, Knowledge database, Debugging, Substitution, Simulation, segmentation, isolation, iteration,
Testing	How do you test the system to prove the system is fixed?	Repeat step 1-2 , Faction testing, and Performance testing
Prevention	What prevention you can put in place to avoid the same problem?	preventive maintenance plan and change management

01

Summarise the process and importance of troubleshooting network faults and implementing recovery actions in five steps.

02

What system unitalities (tools or commands) have you used so far?

03

How did you document configuration information, fault-finding history and remediation action?

Discussion:

Trouble shooting documentation

Site Preparation and Maintenance Records

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/hw/nexus7000/installation/guide/b_n7710_hardware_install_guide/b_n7710_hardware_install_guide_appendix_01010.html

4.1 Restore work-site to safe condition according to established safety procedures

4.2 Record and store essential implementation information according to enterprise procedures

4.3 Notify appropriate personnel of completion of the task according to enterprise procedures

System documentation and record keeping

System documentation

Function requirements,

System capabilities can benchmark

System constrains

Design documentation

Current configuration

Maintenance log and manual.

System backup and recovery schedule – to main and impove the health of the system and prevent future faults and issues.

- Trouble shooting documentation
- Symptoms
- Causes
- Optional: Triggers
- Solutions/resources
- Changes
- Testing results

A (knowledge) Database of problems/recommendation or solutions

Problem ID	Symptom	Area	Category	Possible Causes	Severity	Remediation action	Responsible person

Summary of fault finding methods

Model based – base on framework, structure of abnormal cases/abnormal cases or benchmarks

Knowledge database– use a process to go through testing steps.

Debugging – observe the dynamic process of the system,

Substitution – replace some part or components to see the results

Simulation – rebuild a system of the same function and see the difference.

Testing methods

Faction testing:

- Unit testing.
- Integration testing.
- System testing.
- Acceptance testing.

Performance testing

- Load testing
- Compatibility testing
- Security testing
- Reliability testing

Commonly used tools -networking

- Ping
- Tracert
- NetStat
- NSLookup

  And

- Show ip interface brief
- Show interface
- Show ip access-list
- Show ip route

Commonly used tools - other

WiFi testing tool- WiFi Analyzer.

Wireshark **-** network analysis tools that support packet and protocol analysis

JDisc Discovery **-** scans every device on a network

Addressing for IP networks

Learning outcomes

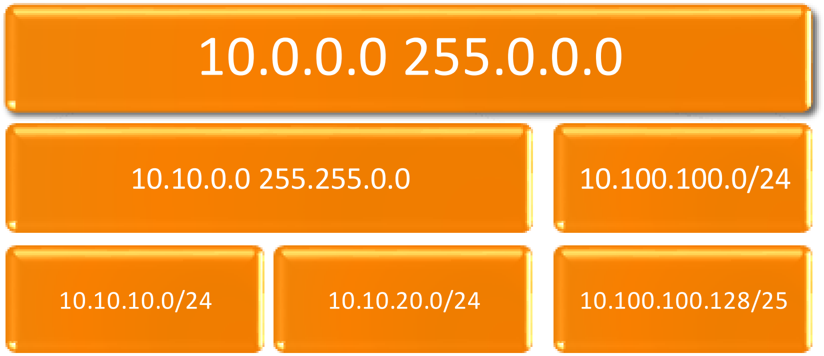
- Understand subnetworks, why do we need subnet masks, and different notations.
- Quickly work out subnet masks for networks of any sizes.
- Understand network ID and broadcasting address and recognise whether two IP addresses are from the same network or not

IP addressing for sub networking

- We have networks of different sizes

- IP address (v4) resources are limited

- Each network have its own “network ID”. We need to know if an Ip addresses belongs to my local network or a “foreign” network.



Hierarchical addressing your network for vlans

Business function	Vlan	Network ID	Subnet masks	Gateway	Size
Marking	10	192.168.1.0	255.255.255.192	192.168.1.1	64
HR	20	192.168.1.64	255.255.255.192	192.168.1.65	64
Accounting	30	192.168.1.128	255.255.255.192	192.168.1.129	64
Admin	40	192.168.1.192	255.255.255.192	192.168.1.193	64

The whole organisation:

192.168.1.0 255.255.255.0 or /24

2. IP addressing for Internetworking and intranetworking

Two networks on two sides of the router: 192.168.1.x and 192.168.2.x

For network A 192.168.1.x:

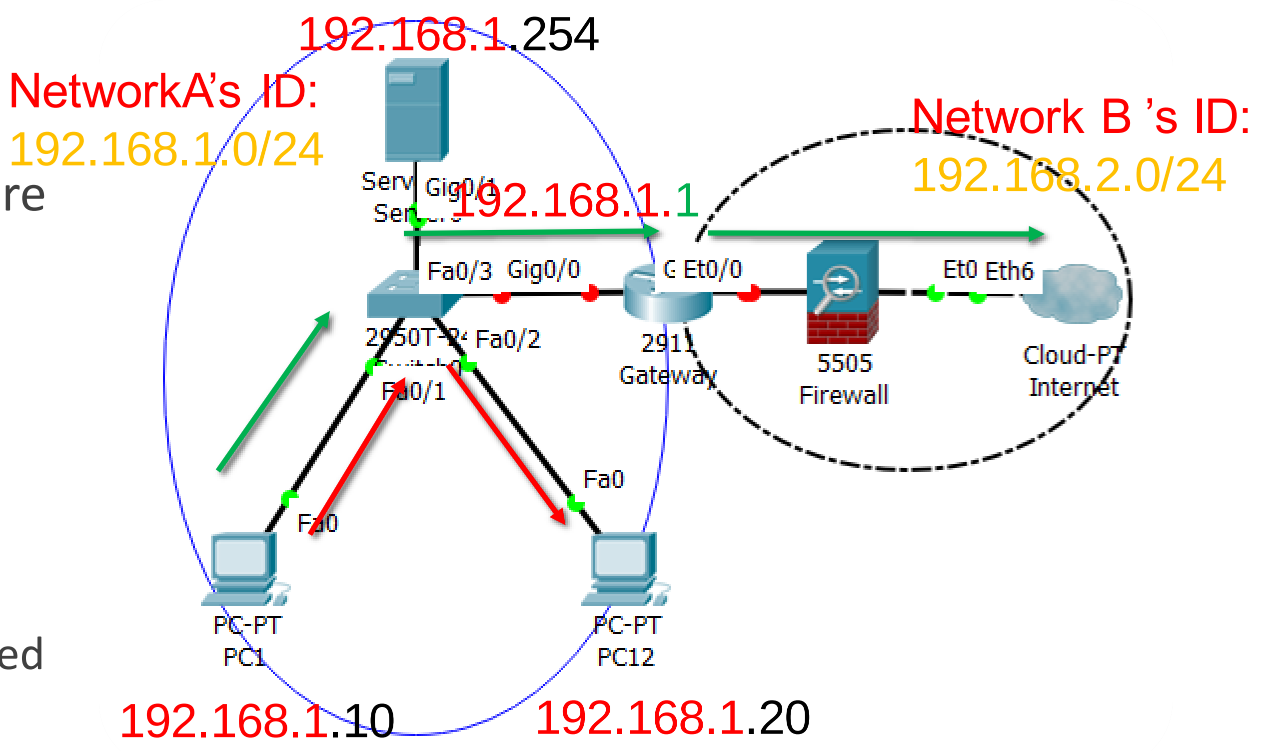
This portion 192.168.1. are fixed. .0 -.255 are open.

However, two Ip addresses are reserved:

- The first : 192.168.1.0 is its network ID:
- The last : 192.168.1.255 is its broadcasting addressee.

Then you have 254 usable Host IDs:

- The first usable ID 192.168.1.1 is typically used as the **gateway address**
- Three computers (PC1, PC2 and the server) use .192.168.1.10, .20, .254



Terminology - IP addressing scheme

IP Address—The unique layer 3 addresses assigned to one host or interface in a network.

Subnet(work) - **A **segment of a network sharing a particular subnet address ("Network ID", e.g. 192.168.10.0).

Subnet mask—A number used to describe which portion of an address refers to the subnet and which part refers to the host, e.g.

- /24,
- 255.255.255.0
- (or wildcard 0.0.0.255)

- You might also have Gateway address and DNS addresses.

Wildcard can be simply calculated from 255.255.255.255 – subnet mask: e.g. 255.255.255.255 – 255.255.255.0 = 0.0.0.255

Reserved IP address

Reserve the following IP addresses within a network :

- The very first one for **Network IDs** (all binary 0s)
- The very last one for **Broadcasting address** (all binary are 1s)
- If you have n bits for host IDs, you will have $2^n - 2$ **usable IP addresses**.
- Many vendors choose the first usable address as the gateway address, e.g. 192.168.1.1 255.255.255.0
- 127.0.0.1 255.255.255.255 is loopback address that stands for the local host itself, 0.0.0.0 0.0.0.0 stands for the whole internet.
- Some other reserved IP addresses: e.g. 224.x.x.x (reserved for multicasting)

x stands for number between 0-255 and 0 as the network ID and 255 as the broad casting address (e.g. 10.255.255.255, 172.16.255.255, 192.168.10.255)

Reserved IP address - Private IP Address and examples

Private IP address can be reused; therefore they are not supposed to appear in the public domain – internet

A /8: (16,777,216 IP addresses) 10.0.0.0 - 10.255.255.255

Network summary 10.x.x.x 255.0.0.0, **wildcard** 0.0.0.255

B /16: (1,048,576 IP addresses) 172.16.0.0- 172.31.255.255.

Network summary address: 172.16.0.0 255.240.0.0 **wildcard** 0.15.255.255

C /24: (65,536 IP addresses) 192.168.0.0- 192.168.255.255; common mask 255.255.255.0,

Network summary address for ACL: 192.168.0.0 255.255.0.0 **wildcard** 0.0.255.255

x stands for number between 0-255 and 0 as the network ID and 255 as the broad casting address (e.g. 10.255.255.255, 172.16.255.255, 192.168.10.255

Why subnet masks? - the lengths of “area IDs” determine the sizes

What is the “area code“, which part is the actual personal number? !

61 3 5022 3720 ->61 0 0000 0000 to 61 9 9999 9999 1,0 00,00 0,000 phone numbers

61 3 5022 3720 ->61 3 0000 0000 to 61 9 9999 9999 10 0,00 0,000 phone numbers

61 3 5022 3720 ->61 3 5000 0000 to 61 3 5999 9999 10 0,00 0,000 phone numbers

61 3 5022 3720 ->61 3 50200 0000 to 61 3 5029 9999 10 0,000 phone numbers

61 3 5022 3720 -> 61 3 5022 0000 to 61 3 5022 9999 10,000 phone numbers

Why subnet masks? – single Area or multi-areas

Person, number, street, suburb, city, state, country,

03 5022 3720

03 5022 3720

How much information can you get from this number?

Why subnet masks? – IP addressing and Sub-networking

Sub-networking – in an IP address, how can we know which network an IP addresses belongs?

Which part is the network's ID, which part is for a specific computer?

192.168.1.10

192.168.1.10

192.168.1 | 10

We need **subnet mask** to tell us that "10" is the computer's address (Host ID) and "192.168.1." is the Network ID (Fixed).

204.17.5.0 - 11001100.00010001.00000101.00000000 (Ip address)
255.255.255.224 - 11111111.11111111.11111111.11100000 (subnet mask)

Why subnet masks? – Classful addresses and subnet masks– A, B, C

Class **Address Range**

Class A 1.0.0.1 to 126.255.255.254 **255.0.0.0 /8** 126 networks 16,777,214 ip addresses/ each network

Class B 128.1.0.1 to 191.255.255.254 **255.255.0.0/16** 16384 networks, 65534 hosts / each network

Class C 192.0.1.1 to 223.255.254.254 **255.255.255.0 /24** 2097152 networks, 256 ip addresses / each network

Why subnet masks? – Classless addresses and variable length subnet masks (VLSM)

Q1. How about networks of other sizes,e.g. 2, 29, 500, etc?

Class C: 192.168.10.100 55.255.255.0 /24

Class B: 192.168.10.100 255.255.0.0 /16

Class A: 192.168.10.100 255.0.0.0 /8

Q2. Do these 192.168.10.100s have the same **network ID**?

192.168.10.100 255.255.252.0 /23
192.168.10.100 255.255.255.252 /30
192.168.10.100 255.255.255.196 /26
192.168.10.100 255.255.255.128 /25

Why subnet masks? – Between class A, B, and C, VLSM

255.0.0.0	/8	
255.255.0.0	/16	
255.255.248.0	**/22**	**1028**
255.255.252.0	**/23**	**512**
255.255.255.0	/24	256
255.255.255.128	**/25**	**128**
255.255.255.196	**/26**	**64**
255.255.255.224	**/27**	**32**
255.255.255.240	**/28**	**16**
255.255.255.248	**/29**	**8**
255.255.255.252	**/30**	**4**

What is the "area code", which part is the actual personal number? !

61 3 5022 3720 ->61 0 0000 0000 to 61 9 9999 9999 1,0 00,00 0,000 phone numbers

61 3 5022 3720 ->61 3 0000 0000 to 61 9 9999 9999 10 0,00 0,000 phone numbers

61 3 5022 3720 ->61 3 5000 0000 to 61 3 5999 9999 10 0,00 0,000 phone numbers

61 3 5022 3720 ->61 3 50200 0000 to 61 3 5029 9999 10 0,000 phone numbers

61 3 5022 3720 -> 61 3 5022 0000 to 61 3 5022 9999 10,000 phone numbers

01

Why do we need subnetworks, why do we need subnet masks?

02

Are“/27” or 255.255.255.224 the same ? How many times is /27 larger than /28?

03

Which IP address has to be reserved as network ID, which IP address is normally used as gateway address?

Discussion:

Fast IP addressing technique

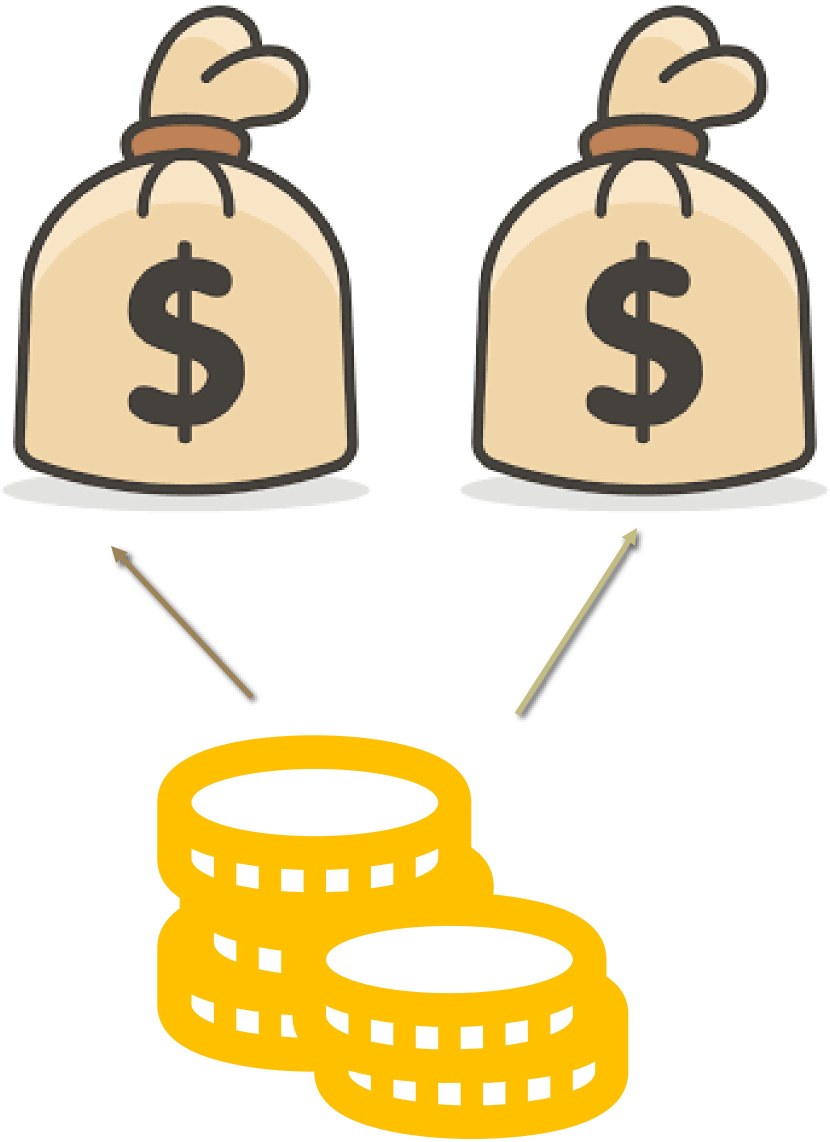
Learning outcomes

- Understand subnetworks, why do we need subnet masks, and different notations.
- Quickly work out subnet masks for networks of any sizes.
- Understand network ID and broadcasting address and recognise whether two IP addresses are from the same network or not

You have 256 dollars, you want to use 32 dollars, how much can you save (224)?

You have 32 gold coins, you want to use 5 to buy something, how many coins can you keep (27)?

In a promotion, if one gold coins can change two dollars, two can change four dollars, three can change eight dollars… how many dollars can above 5 gold coins change?



Binary vs. decimal notations

- The computers use 32 digits (bits) to store IP (v4) addresses.
- They are divided into four groups: 8bits. 8bits. 8bits. 8bits;
- Subnet masks are presented as 1 bits, indicating the bit in the same position of the IP address is fixed as a part of network ID

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**	
1	0	0	1	0	0	1	0	*(146)*
0	1	1	1	0	1	1	1	*(119)*
1	1	1	1	1	1	1	1	

204.17.5.0 - 11001100.00010001.00000101.00000000 (Ip address)
255.255.255.224 - 11111111.11111111.11111111.11100000 (subnet mask)

In this case, out of total 32 bits, 8+8+8+3 = 27 bits are fixed under the subnet mask, 5 bits are open, so you have 32 host IDs. Then you have 224 addresses fixed. Therefore the subnet mask is 255.255.255.224

https://www.youtube.com/watch?v=LxNgWsseE0w

https://www.youtube.com/watch?v=XQ3T14SIlV4

How bits “make” decimal numbers? The Story of 2^x

2^x

1 coin: 2

2 coins: 4

3 coins: 8

4 coins: 16

5 coins: 32

6 coins: 64

7 coins: 128

8 coins: 256

1+8 coins: 512

2+8 coins: 1024

3+8 coins: 2048

....

Note: for networks lager than class C "/24", you need all 8 bits in the last group plus some more in the third group.

Or, 1 gold coin buys 2 IP addresses...

The two notations: fixed and open

To subdivide your network to suit smaller networks, you can fix more bits and open less. E.g. for a group that has 20 users, the size of the network can be 32 (why?). You open 32 host IDs (or 5 bits). Accordingly you fix 224 IDs (or 27 bits)

You open 5 bits, which can make 2^5=32 IP addresses

$\underbrace{8b.8b.8b.3b}_{\text{You keep 8+8+8+3 =27 bits under the mask as "Area ID"}}+\overbrace{5b}$

Total: 255.255.255.256

Open: 32

Mask:255.255.255.224

Allocating the 32 bits: fixed vs. open?

8b.8b.8b.3b.+5b ->27+5 = 32

8+8+8+3 =27 bits are under the mask as "Area ID"

you open 5 bits (32 addresses) for hosts

8+8+6 =22 bits are under the mask as "Area ID"

You open 10 bits (1024 addresses) for hosts, including all 8 bits in group 4 and 2 more bits in gourp 3

8b.8b.6b+2b.8b ->22+10 =32

Fixed or open: both notations

255.255.255.224 (+32) - >/27 (+2^5)

/27(24+3) bits for mask, 5 bits for hosts

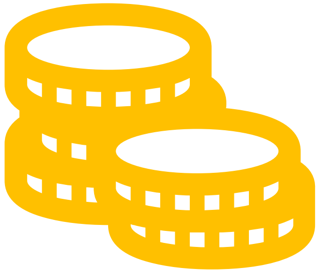
255.255.255.252 (+4) - >/30 (+2^2)

/30 (24+6) bits for mask, 2 bits for hosts

255.255.252.0 (+1024) - >/22 (2^{2+8})

/22 bits for mask, 10 bits (2+8) for hosts

The gold coin game - decimal version (256) or bits version(32)



256 Ip addresses or 8/32 bits

Subnet masks – fixed bits or numbers

Host Ip addresses – opened bits or numbers

Sizes, Ranges, and network IDs

192.168.10.100	**255.255.252.0**	**/23**	512	192.168.8.0 - 192.168.9.255
192.168.10.100	**255.255.255.0**	**/24**	256	192.168.10.0 – 192.168.10.255
…			…	…
192.168.10.100	**255.255.255.224**	**/27**	32	192.168.10.96 - 192.168.10.127
…				
192.168.10.100	**255.255.255.248**	**/29**	8	192.168.10.96 - 192.168.10.103
192.168.10.100	**255.255.255.252**	**/30**	4	192.168.10.100 – 192.168.10.103

192.168.10.0 - 31; 192.168.10.32 –.63; 192.168.10.64 - 95; 192.168.10.96 – 127; 192.168.10.128 – 159; 192.168.10.160 – 195;….

Q1. How about networks of other sizes,e.g. 2, 29, 500, etc?

Q2. Do these 192.168.10.100s have the same **network ID**?

IP addressing dictionary

Fixed bits and open bits	IP addresses	Open IP addresses / Network sizes	Subnet masks	Example of IP Ranges/sub networks
/30 (+2)	2^2	+ 4 IP addrs	255.255.255.252	0-3, 4-7, 8-11, 12-15, 16-19, 20-23, 24-27, 28-31, 32-25..
/29 (+3)	2^3	+ 8 IP addrs	255.255.255.248	0-7,8-15,16-31,32-47,48-63,64-73,74-80,80-95,96-103…
/28 (+4)	2^4	+ 16 IP addrs	255.255.255.240	0-15, 16-31, 32-47, 48-63, 64-79, 80-95, 96-111,112-127…
/27 (+5)	2^5	+ 32 IP addrs	255.255.255.224	0-31, 32- 63, 64-95, 96-127, 128-159, 160-195, 196-227…
/26 (+6)	2^6	+ 64 IP addrs	255.255.255.196	0-63, 64-127, 128-195, 196-255
/25 (+7)	2^7	+ 128 IP addrs	255.255.255.128	0-127, 128-255
/24 (+8)	2^8	+ 256 IP addrs	255.255.255.0	0-255
/23 (+8+1)	2^1*2^8	+ 2*256 IP addrs	255.255.254.0	.0.0-.1.255, .2.0-.3.255, .4.0-.5.255,.6.0-.7.255…
/22 (+8+2)	2^2*2^8	+ 4*256 IP addrs	255.255.252.0	.0.0-.3.255, .4.0-.7.255
…	…	…	…	…

Using hierarchical addressing for vlans

Business function	Vlan	Network ID	Subnet masks	Gateway	Size
Marking	10	192.168.10.0	255.255.255.192	192.168.10.1	64
HR	20	192.168.10.64	255.255.255.192	192.168.10.65	64
Accounting	30	192.168.10.128	255.255.255.192	192.168.10.129	64
Admin	40	192.168.10.196	255.255.255.192	192.168.10.193	64

Hierarchical IP addressing

A classful IP address group can be divided into multiple smaller. The strategies include:

Classless IP address allocate IP addresses with vary length subnet masks (VLSM) that does not fall into any classes.

Addresses can be summarised to the closest classes.

Match IP address groups or sub-networks to virtual local area network memberships

01

Why do we need subnetworks, why do we need subnet masks?

02

If the subnet masks is 255.255.255.224, how many computers can this network have?

03

Are 192.168.1.1 and 192.168.1.10 in the same network when subnet mask is 255.255.255.252

Discussion: hierarchical addressing

Stateless address autoconfiguration (SLAAC)

To perform address configuration on IPv6 we can use :

- static addressing,
- static addressing with DHCPv6 (stateless),
- dynamic addressing via DHCPv6 (Stateful),
- SLAAC alone,
- SLAAC with DHCPv6 (Stateless).

SLAAC can provide address to a host based on a network prefix advertised from a local network router via Router Advertisements (RA).

Extended Unique Identifier (EUI-64) conversion can use the MAC address of an interface to generate a unique 64-bit interface ID. This is to split the MAC address in half and place FF:FE in the middle,

Prefix + :0000:0000: +host identifier

Reference

TGA, Unit of competency details ICTTEN419, https://training.gov.au/Training/Details/ICTTEN419. Retrieved on 4/04/2019

ISO, 35.100 - Open systems interconnection (OSI), https://www.iso.org/ics/35.100/x/ Retrieved on 4/04/2019

Cisco Corp. IP Addressing and Subnetting for New Users. URL://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html Retrieved on 4/02/2015, Retrieved on 4/04/2019

Kaushik Das IPv6 Addressing http://www.ipv6.com/articles/general/IPv6-Addressing.htm Retrieved on 4/02/2015, Retrieved on 4/04/2019

IEFT, Address Allocation for Private Internets

http://tools.ietf.org/html/rfc1918 Retrieved on 4/02/2015

Microsoft Technology Position Paper http://download.microsoft.com/download/e/9/b/e9bd20d3-cc8d-4162-aa60-3aa3abc2b2e9/IPv6.doc Retrieved on 4/02/2015

Reference

Cisco, Configuration Fundamentals - Command-Line Interfaces https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/cli.html Retrieved on 05/08/2016 Retrieved on 4/02/2015

IDC Technologies, Data transmission - Cabling , http://www.idc-online.com/technical_references/pdfs/data_communications/Data_transmission_Cabling.pdf Retrieved on 05/08/2016 Retrieved on 4/02/2015, Retrieved on 4/04/2019

Halmstad University, Routing and Routing Protocols www.hh.se/download/18.2515361d135136944718000773 5/routing retrieved 2/3/2016

Cisco, Cisco Router Architecture http://www.cisco.com/networkers/nw99_pres/601.pdf retrieved 2/3/2016

Cisco, Internetwork Design Guide http://docwiki.cisco.com/wiki/Internetwork_Design_Guide retrieved 2/3/2016

Cisco, EIGRP Stub Routing http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/eigrpstb.html retrieved 2/3/2016

Reference

Cisco Design Guides http://www.cisco.com/c/en/us/tech/ip/ip-routing/tech-design-guides-list.html retrieved 2/3/2016

Basic Router Configuration http://ciscoelearning.blogspot.com.au/2009/03/basic-router-configuration.html, retrieved 2/3/2016

Cisco, asic Router Configuration http://www.cisco.com/c/en/us/td/docs/routers/access/1900/software/configuration/guide/Software_Configuration/routconf.html#15062, retrieved 2/3/2016

How to: Backup Cisco IOS image to TFTP server http://www.kiwisyslog.com/help/cattools/index.html?act_devclisendcmd_howtobackup.htm, retrieved 2/3/2016

Cisco, http://www.cisco.com/c/en/us/td/docs/switches/datacenter/hw/nexus7000/installation/guide/b_n7710_hardware_install_guide/b_n7710_hardware_install_guide_chapter_010.html Retrieved 06/07/2017

Cisco,http://www.cisco.com/c/en/us/td/docs/switches/datacenter/hw/nexus7000/installation/guide/b_n7710_hardware_install_guide/b_n7710_hardware_install_guide_chapter_0101.html Retrieved 06/07/2017

Cisco,http://www.cisco.com/c/en/us/td/docs/routers/7600/Hardware/Chassis_Installation/7600_Series_Router_Installation_Guide/cis_76xx/0bcabcon.html Retrieved 06/07/2017