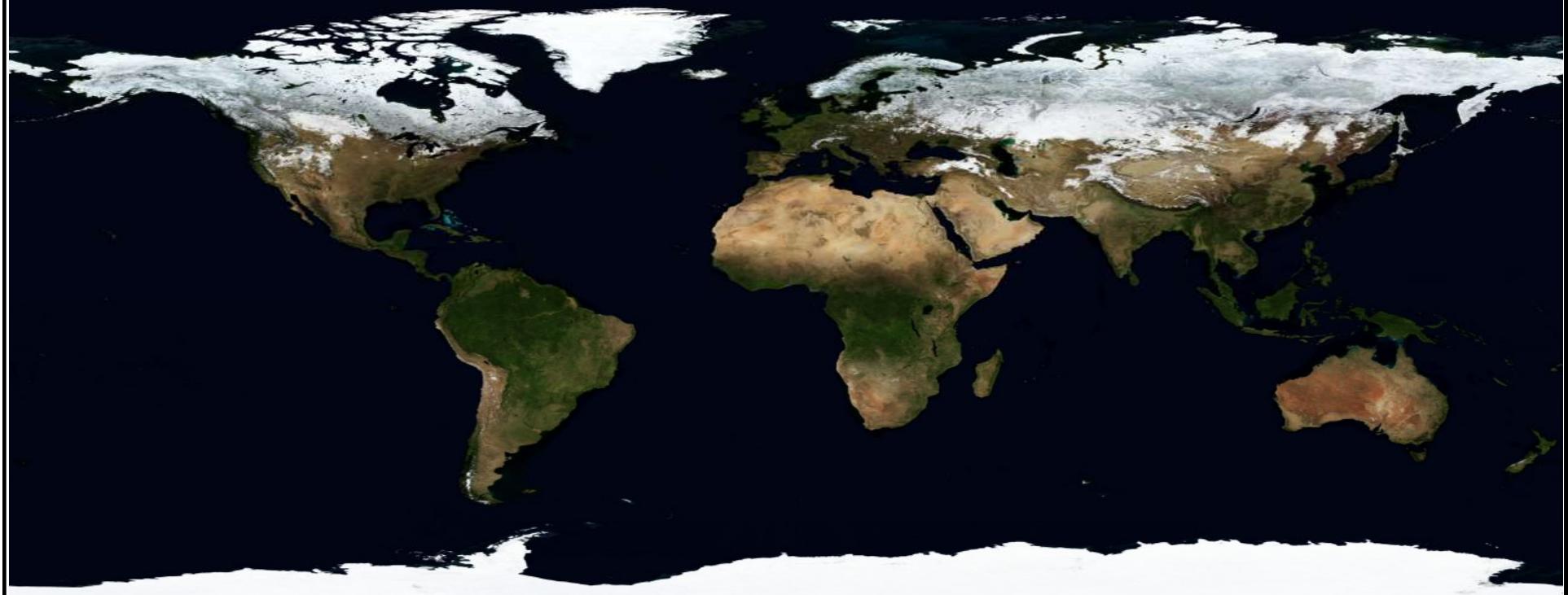


CCNA_R&S_200-125

Concept/Practice/Troubleshooting



AI Research Team: Thilaga & kumar.

Version: 2.1

Created on: Wednesday, DEC 23, 2014

Last Lesson Learned on : Thursday, March 28, 2019



kumar6009@gmail.com



@air.ds2

Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3

Ground Rules

- Quality = Time + Scope + Cost Management
- Please switch-off or silence your mobiles/Laptops
 - **Call On Demand: Please go out the class & attend the Mobile calls/what's up**
- If you are absent to class, please inform the instructor/counselors
- For ID Card, Books {Hard & Soft}, Exam, Backup Class {Theory/Lab}, Placements, Leaves & Holidays
 - – Contact Front Desk {Management}
 - **SPOC: Counselor, Batch Scheduler & Lab In-charge**
- Note all yours questions:
 - While Teaching, Please focus on the topics on the class
 - Other than the course syllabus, We will discuss all questions in Q&A session {15 Mins}



*Live as if you were
to die tomorrow.
Learn as if you were
to live forever.*

© 2009 Inspiration 4D International Ltd

- | | |
|--|--|
| 1. Network Fundamentals <ul style="list-style-type: none"> ➤ 1. OSI and TCP/IP models, ➤ 2. TCP/IP Protocol Suite –TCP, UDP, IPv4, IPv6 & Ethernet, ➤ 3. Enterprise network Infrastructure Design– Firewalls, Access points, Wireless controllers, cloud, collapsed core and three-tier arch, ➤ 4. Topologies, Cable & Connectors, troubleshooting methodologies. ➤ 5. Addressing Format, {Port add, MAC add, IPv4 addressing Basics , Public vs. Private, CIDR to Subnet Mask Conversion} ➤ 6. Subnetting - Class C, B, A & VLSM & IPv6 Basics | 4. Infrastructure Services <ul style="list-style-type: none"> ➤ 15. ACL, NAT ➤ 17. HSRP ➤ 18. DNS, DHCP, NTP |
| 2. LAN Switching Technologies <ul style="list-style-type: none"> ➤ 7. NW Devices: Purpose & Functions, BD/CD Exercise, ➤ 8. IOS Basics{LAB01}, Telnet, SSH & SW MGT IP ➤ 9. VLAN, Trunk, VTP, 10. STP, PVSTP, RSTP, ➤ 11.L2/L3 Ether channel & Inter-VLAN Routing | 5. Infrastructure Security <ul style="list-style-type: none"> ➤ 19. Terminologies ➤ 20. 802.1x, DHCP Snooping Attack ➤ 21. APIC-EM ACL Path Trace tool ➤ 22. SW-Port Security ➤ 23. AAA {Radius & TACACS+} |
| 3. Routing Technologies <ul style="list-style-type: none"> ➤ 10. Static Routing {NW Route, Host Route, Default Route, Floating Route}, ➤ 11. RIPv2, EIGRP, ➤ 12. OSPF-Single-area, ➤ 13. OSPF-Multiarea, ➤ 14. IPv6-Static, OSPF, EIGRP, RIPng | 6. Infrastructure Management <ul style="list-style-type: none"> ➤ 24. SNMP, SYSLOG, Backup & Restore ➤ 25. CDP / LLDP, TFTP, PSSWD Recovery, ➤ 26. Terminal Monitor, SPAN |
| | 7. WAN {SP} Technologies <ul style="list-style-type: none"> ➤ 27. OSI Model, Physical, Types , HDLC, PPP {PAP, CHAP, MLPPP, PPPoE}, ➤ 28. QOS ➤ 29. Network Programmability , ➤ 30. VPN {GRE}, eBGP |

Table of Contents

0. Ground Rules

15% 1.0 Network Fundamentals

1.1 Compare and contrast OSI and TCP/IP models

1.2 Compare and contrast TCP and UDP protocols

1.3 Describe the impact of infrastructure components in an enterprise network

1.3.a Firewalls

1.3.b Access points

1.3.c Wireless controllers

1.4 Describe the effects of cloud resources on enterprise network architecture

1.4.a Traffic path to internal and external cloud services

1.4.b Virtual services

1.4.c Basic virtual network infrastructure

1.5 Compare and contrast collapsed core and three-tier architectures

1.6 Compare and contrast network topologies

1.6.a Star

1.6.b Mesh

1.6.c Hybrid

1.7 Select the appropriate cabling type based on implementation requirements

1.8 Apply troubleshooting methodologies to resolve problems

1.8.a Perform and document fault isolation

1.8.b Resolve or escalate

1.8.c Verify and monitor resolution

1.9 Configure, verify, and troubleshoot IPv4 addressing and subnetting

1.10 Compare and contrast IPv4 address types

1.10.a Unicast

1.10.b Broadcast

1.10.c Multicast

1.11 Describe the need for private IPv4 addressing

1.12 Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment

1.13 Configure, verify, and troubleshoot IPv6 addressing

1.14 Configure and verify IPv6 Stateless Address Auto Configuration

1.15 Compare and contrast IPv6 address types

1.15.a Global unicast

1.15.b Unique local

1.15.c Link local

1.15.d Multicast

1.15.e Modified EUI 64

1.15.f Autoconfiguration

1.15.g Anycast

S/N	Topics	Percentage	Hours	Sessions
1	Network Fundamentals	15	6	3
2	LAN Switching Technologies	21	8.4	4
3	Routing Technologies	23	9.2	5
4	WAN Technologies	10	4	2
5	Infrastructure Services	10	4	2
6	Infrastructure Security	11	4.4	2
7	Infrastructure Management	10	4	2
Grand Total >>		100	40	20



Table of Contents

21% 2.0 LAN Switching Technologies

2.1 Describe and verify switching concepts

- 2.1.a MAC learning and aging
- 2.1.b Frame switching
- 2.1.c Frame flooding
- 2.1.d MAC address table

2.2 Interpret Ethernet frame format

2.3 Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

2.4 Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

- 2.4.a Access ports (data and voice)
- 2.4.b Default VLAN

2.5 Configure, verify, and troubleshoot interswitch connectivity

- 2.5.a Trunk ports
- 2.5.b Add and remove VLANs on a trunk
- 2.5.c DTP, VTP (v1&v2), and 802.1Q
- 2.5.d Native VLAN

2.6 Configure, verify, and troubleshoot STP protocols

- 2.6.a STP mode (PVST+ and RPVST+)
- 2.6.b STP root bridge selection

2.7 Configure, verify and troubleshoot STP related optional features

- 2.7.a PortFast
- 2.7.b BPDU guard

2.8 Configure and verify Layer 2 protocols

- 2.8.a Cisco Discovery Protocol
- 2.8.b LLDP

2.9 Configure, verify, and troubleshoot (Layer 2/Layer 3) EtherChannel

- 2.9.a Static
- 2.9.b PAGP
- 2.9.c LACP

2.10 Describe the benefits of switch stacking and chassis aggregation

S/N	Topics	Percentage	Hours	Sessions
1	Network Fundamentals	15	6	3
2	LAN Switching Technologies	21	8.4	4
3	Routing Technologies	23	9.2	5
4	WAN Technologies	10	4	2
5	Infrastructure Services	10	4	2
6	Infrastructure Security	11	4.4	2
7	Infrastructure Management	10	4	2
Grand Total >>		100	40	20



Table of Contents

23% 3.0 Routing Technologies

3.1 Describe the routing concepts

- 3.1.a Packet handling along the path through a network
- 3.1.b Forwarding decision based on route lookup
- 3.1.c Frame rewrite

3.2 Interpret the components of a routing table

- 3.2.a Prefix
- 3.2.b Network mask
- 3.2.c Next hop
- 3.2.d Routing protocol code
- 3.2.e Administrative distance
- 3.2.f Metric
- 3.2.g Gateway of last resort

3.3 Describe how a routing table is populated by different routing information sources

- 3.3.a Admin distance

3.4 Configure, verify, and troubleshoot inter-VLAN routing

- 3.4.a Router on a stick
- 3.4.b SVI

3.5 Compare and contrast static routing and dynamic routing

3.6 Compare and contrast distance vector and link state routing protocols

3.7 Compare and contrast interior and exterior routing protocols

3.8 Configure, verify, and troubleshoot IPv4 and IPv6 static routing

- 3.8.a Default route
- 3.8.b Network route
- 3.8.c Host route
- 3.8.d Floating static

3.9 Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

3.10 Configure, verify, and troubleshoot single area and multi-area OSPFv3 for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

3.11 Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

3.12 Configure, verify, and troubleshoot EIGRP for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub)

3.13 Configure, verify, and troubleshoot RIPv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution)

3.14 Troubleshoot basic Layer 3 end-to-end connectivity issues

S/N	Topics	Percentage	Hours	Sessions
1	Network Fundamentals	15	6	3
2	LAN Switching Technologies	21	8.4	4
3	Routing Technologies	23	9.2	5
4	WAN Technologies	10	4	2
5	Infrastructure Services	10	4	2
6	Infrastructure Security	11	4.4	2
7	Infrastructure Management	10	4	2
Grand Total >>>		100	40	20



Table of Contents

10% 4.0 WAN Technologies

4.1 Configure and verify PPP and MLPPP on WAN interfaces using local authentication

4.2 Configure, verify, and troubleshoot PPPoE client-side interfaces using local authentication

4.3 Configure, verify, and troubleshoot GRE tunnel connectivity

4.4 Describe WAN topology options

- 4.4.a Point-to-point
- 4.4.b Hub and spoke
- 4.4.c Full mesh
- 4.4.d Single vs dual-homed

4.5 Describe WAN access connectivity options

- 4.5.a MPLS
- 4.5.b Metro Ethernet
- 4.5.c Broadband PPPoE
- 4.5.d Internet VPN (DMVPN, site-to-site VPN, client VPN)

4.6 Configure and verify single-homed branch connectivity using eBGP IPv4 (limited to peering and route advertisement using Network command only)

4.7 Describe basic QoS concepts

- 4.7.a Marking
- 4.7.b Device trust
- 4.7.c Prioritization
 - 4.7.c. (i) Voice
 - 4.7.c. (ii) Video
 - 4.7.c. (iii) Data
- 4.7.d Shaping
- 4.7.e Policing
- 4.7.f Congestion management

S/N	Topics	Percentage	Hours	Sessions
1	Network Fundamentals	15	6	3
2	LAN Switching Technologies	21	8.4	4
3	Routing Technologies	23	9.2	5
4	WAN Technologies	10	4	2
5	Infrastructure Services	10	4	2
6	Infrastructure Security	11	4.4	2
7	Infrastructure Management	10	4	2
Grand Total >>		100	40	20



Table of Contents

10% 5.0 Infrastructure Services

5.1 Describe DNS lookup operation

5.2 Troubleshoot client connectivity issues involving DNS

5.3 Configure and verify DHCP on a router (excluding static reservations)

5.3.a Server

5.3.b Relay

5.3.c Client

5.3.d TFTP, DNS, and gateway options

5.4 Troubleshoot client- and router-based DHCP connectivity issues

5.5 Configure, verify, and troubleshoot basic HSRP

5.5.a Priority

5.5.b Preemption

5.5.c Version

5.6 Configure, verify, and troubleshoot inside source NAT

5.6.a Static

5.6.b Pool

5.6.c PAT

5.7 Configure and verify NTP operating in a client/server mode

S/N	Topics	Percentage	Hours	Sessions
1	Network Fundamentals	15	6	3
2	LAN Switching Technologies	21	8.4	4
3	Routing Technologies	23	9.2	5
4	WAN Technologies	10	4	2
5	Infrastructure Services	10	4	2
6	Infrastructure Security	11	4.4	2
7	Infrastructure Management	10	4	2
Grand Total >>		100	40	20



Table of Contents

11% 6.0 Infrastructure Security

6.1 Configure, verify, and troubleshoot port security

- 6.1.a Static
- 6.1.b Dynamic
- 6.1.c Sticky
- 6.1.d Max MAC addresses
- 6.1.e Violation actions
- 6.1.f Err-disable recovery

6.2 Describe common access layer threat mitigation techniques

- 6.2.a 802.1x
- 6.2.b DHCP snooping
- 6.2.c Nondefault native VLAN

6.3 Configure, verify, and troubleshoot IPv4 and IPv6 access list for traffic filtering

- 6.3.a Standard
- 6.3.b Extended
- 6.3.c Named

6.4 Verify ACLs using the APIC-EM Path Trace ACL Analysis tool

6.5 Configure, verify, and troubleshoot basic device hardening

- 6.5.a Local authentication
- 6.5.b Secure password
- 6.5.c Access to device
- 6.5.c. (i) Source address
- 6.5.c. (ii) Telnet/SSH
- 6.5.d Login banner

6.6 Describe device security using AAA with TACACS+ and RADIUS

S/N	Topics	Percentage	Hours	Sessions
1	Network Fundamentals	15	6	3
2	LAN Switching Technologies	21	8.4	4
3	Routing Technologies	23	9.2	5
4	WAN Technologies	10	4	2
5	Infrastructure Services	10	4	2
6	Infrastructure Security	11	4.4	2
7	Infrastructure Management	10	4	2
Grand Total >>>		100	40	20



Table of Contents

10% 7.0 Infrastructure Management

7.1 Configure and verify device-monitoring protocols

- 7.1.a SNMPv2
- 7.1.b SNMPv3
- 7.1.c Syslog

7.2 Troubleshoot network connectivity issues using ICMP echo-based IP SLA

7.3 Configure and verify device management

- 7.3.a Backup and restore device configuration
- 7.3.b Using Cisco Discovery Protocol or LLDP for device discovery
- 7.3.c Licensing
- 7.3.d Logging
- 7.3.e Timezone
- 7.3.f Loopback

7.4 Configure and verify initial device configuration

7.5 Perform device maintenance

- 7.5.a Cisco IOS upgrades and recovery (SCP, FTP, TFTP, and MD5 verify)
- 7.5.b Password recovery and configuration register
- 7.5.c File system management
- 7.6 Use Cisco IOS tools to troubleshoot and resolve problems
- 7.6.a Ping and traceroute with extended option
- 7.6.b Terminal monitor
- 7.6.c Log events
- 7.6.d Local SPAN

S/N	Topics	Percentage	Hours	Sessions
1	Network Fundamentals	15	6	3
2	LAN Switching Technologies	21	8.4	4
3	Routing Technologies	23	9.2	5
4	WAN Technologies	10	4	2
5	Infrastructure Services	10	4	2
6	Infrastructure Security	11	4.4	2
7	Infrastructure Management	10	4	2
Grand Total >>>		100	40	20

7.7 Describe network programmability in enterprise network architecture

- 7.7.a Function of a controller
- 7.7.b Separation of control plane and data plane
- 7.7.c Northbound and southbound APIs



CCNA R&S – 200-125 - Lab Details >>

[Lab 01 - IOS Basics](#) [152]
[Lab 02 - Telnet](#) [VTY line] [158]
[Lab 03 – SSH](#) [VTY line] [158]
[Lab 04 - Switching - MGT IP](#) [158]
[Lab 05 – VLAN](#) [181]
[Lab 06 – TRUNK](#) [181]
[Lab 07 – VTP](#) [181]
[Lab 08 - Port Fast](#) [194]
[Lab 09 - Root Bridge](#) [194]
[Lab 10 - RSTP](#) [194]
[Lab 11 - PVSTP+](#) [194]
[Lab 12 - BPDU guard](#)[GNS3] [194]
[Lab 13 – CDP](#) [194]
[Lab 14 - LLDP](#) [Real– TTY] [218]
[Lab 15 - L2 EC - Static](#) [222]
[Lab 16 - L2 EC - PAGP](#) [222]
[Lab 17 - L2 EC - LACP](#) [222]
[Lab 18 - L3 EC - Static](#) [222]
[Lab 19 - L3 EC - PAGP](#) [222]
[Lab 20 - L3 EC - LACP](#) [222]

[Lab 21 - Router on stick](#) [235]
[Lab 22 - L3 Switching](#) [239]
[Lab 23 – Routing - Serial](#) [248]
[Lab 24 - Static - Host route](#) [248]
[Lab 25 – Static: NW route](#) [248]
[Lab 26 - Static:Default route](#) [248]
[Lab 27:Static :Floating route](#) [248]
[Lab 28 - RIPv2](#) [248]
[Lab 29 – EIGRP](#) [282]
[Lab 30 - OSPF Single Area](#) [297]
[Lab 31 - OSPF Multi Area](#) [306]
[Lab 32 - IPv6 – Serial/Static](#) [288]
[Lab 33 - IPv6 – OSPF](#) [288]
[Lab 34 - IPv6 - EIGRP](#) [288]
[Lab 35:Services: ACL N:STD](#) [318]
[Lab 36 - ACL NUM-EXT](#) [324]
[Lab 37 - ACL NAME_STD](#) [324]
[Lab 38 :ACL IPv6:NAME EXT](#) [331]
[Lab 39 – DHCP](#) [GNS3] [336]
[Lab 40 – HSRP](#) [344]

[Lab 41 - NAT – Static](#) [349]
[Lab 42 - NAT – Pool](#) [349]
[Lab 43 - NAT – PAT](#) [349]
[Lab 44 - NTP](#) [361]
[Lab 45 - WAN – PPP](#) [376]
[Lab 46 – CHAP](#) [378]
[Lab 47 - MLPPP](#) [GNS3] [380]
[Lab 48 - GRE](#) [GNS3] [393]
[Lab 49 – eBGP](#) [GNS3] [403]
[Lab 50 - Security – AAA](#) [361]
[Lab 51 - SW port SEC](#) [429]
[Lab 52 - MGT:SYSLOG](#) [361]
[Lab 53 - IPSLA](#) [GNS3] [441]
[Lab 54 - IOS Licensing](#) [361]
[Lab 55 - ROU psswd rec](#) [361]
[Lab 56 - TFTP](#) [361]
Lab 57 - Reserved for R&D
Lab 58 - Reserved for R&D
Lab 59 - Reserved for R&D
Lab 60 - Reserved for R&D



Introduction

Lesson 1



Table of Contents

- Name, Education & Networking{IT} Experience
- Contents at a glance: Information Technology [IT]
- Cisco Certifications [Levels & Tracks]
- Certifications :Core, Advanced, On-Demand & Design?
- How do we train?
- Levels of Knowledge
- Types of Learning
- Intended Audience
- Pre-Requisites, Lab Requirements, Duration
- CCNA R&S Syllabus , flow
- How to get the most of this course? i.e. Lab Details



Name, Education & IT Experience



NAME : KUMAR ; ADACEMIC EDUCATION: Diploma in Electronics & Communication {DECE}

INFORMATION TECHNOLOGY {IT} EXPERIENCE: 20+ years

- 1994
 - Student – Software course - Basic DOS, FoxPro & Clipper
 - Part Time – Jayashree Electronics, Madurai, India
- 1997 – 2001
 - Entrepreneur – Proprietor in Vinayaga Electronics, Madurai, India
 - Diploma in Desktop Publishing & Radio/Tape Recorder/TV/VCR & Computer Hardware {chip level}
- 2001 – 2002
 - Resident Engineer in Vel Computers Pvt. Ltd. , Tamilnadu{Partly} & Karnataka, India
 - Hardware, Networking, Novel Netware + Windows systems administration
- 2002 - 2003
 - Customer Support Executive in Mark Computers Services, Mysore, India
 - MCSE 2000, Unix, Linux , Sun Solaris & CCNA
- 2003 – 2005
 - Consultant – Professional Services in IBM {Network Solutions Pvt. Ltd}, Bangalore, India
- 2005 – 2006
 - Network Specialist – Performance Engineering in Intel Corporation , Bangalore, India
- Researcher - Artificial Intelligence-Research & Development
 - ai R&D Stage 1 – Basic Research - Since Jan 2005
 - 2005-2007 - Technical Head in IIHT, Chennai, India + Freelancer
 - 2007-2009 - IT Consultant in eGestalt , Bangalore, India
 - 2010-2014 - Freelancer + Finishing ai R&D Stage 1 - Basic Research
 - ai R&D Stage 2 – Applied Research - Since July, 2014 - GIT >> Techno-BDM
 - Role: Instructor i.e. Teaching A+, N+, SEC+, CCNA{R&S, SEC & WiFi}, CCNP {R&S}, ITIL {FND} & CISSP
 - Responsibilities: Admin, Sales & Marketing, Remote Lab Support, Retail, Corporate*(MNC), Colleges & Online Trainings



Mission Milestones = S+, MCSE Cloud, RHCE Open stack , VCP-DCV, Python, CEH, CCDA, CCIE{R&S, SEC, DC & Collaboration} & MBA {HR & Finance}



kumar6009@gmail.com



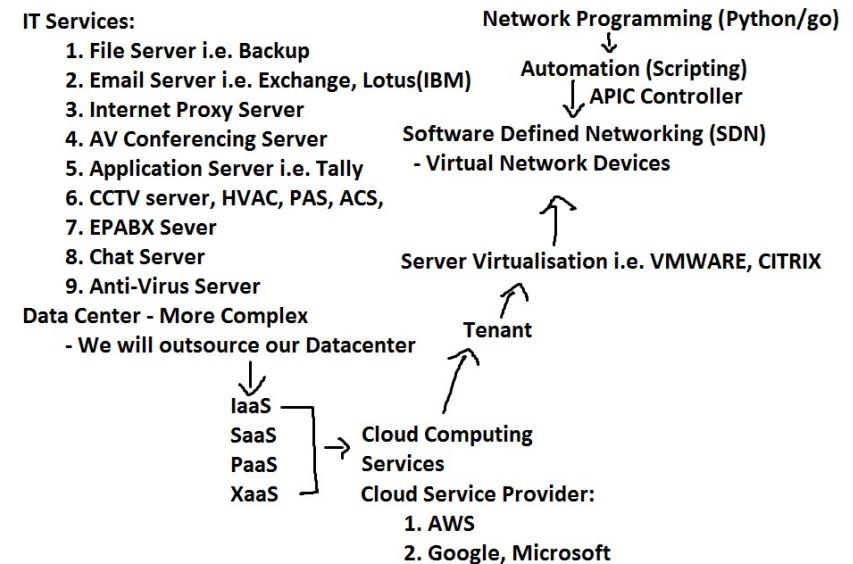
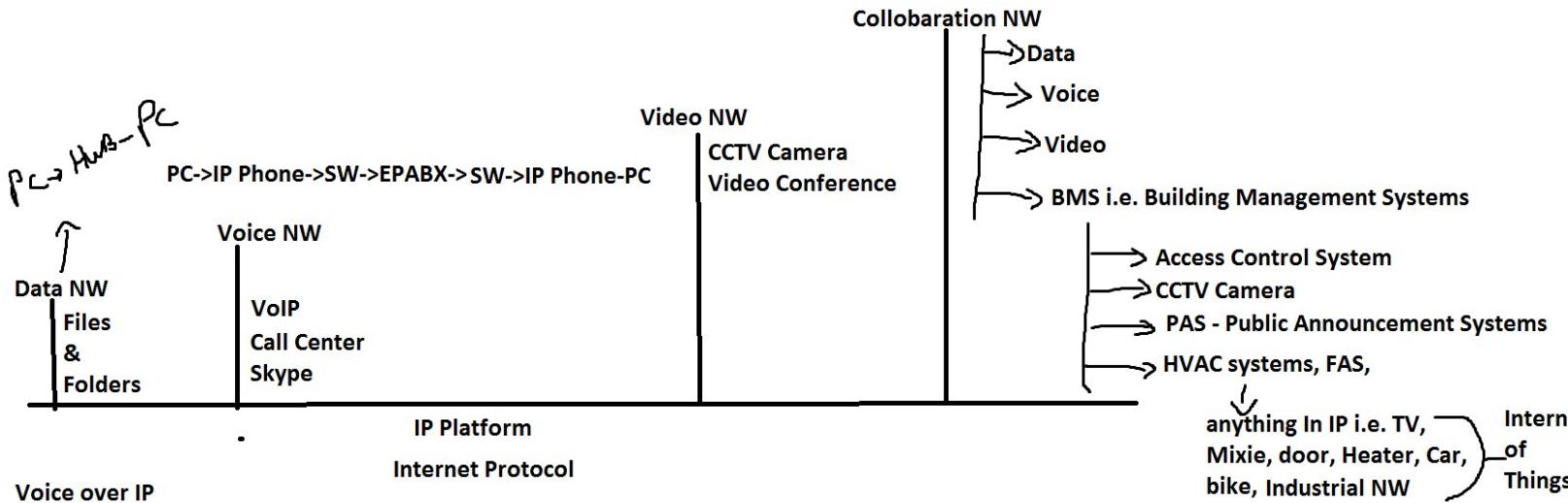
@air.ds2

Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3

14

Evolution of IT



Steps in IT Career



Learning is a eternal process



4th **CCAr {The Architect}**
- ITIL/CISSP/CHFI/MBA

3rd **CCIE (R&S, SEC, WIFI, SP, DC, CO, Cloud)**

2nd **CCNP & Specialist Certifications/CEH**

1st **CCNA {R&S, Security, Wireless, Service Provider, DC}**

UKG **CompTIA N+ {Networking- Architecture, operations, security & TS }
- Theory - Topology, OSI Layers, IPv4(CIDR, VLSM), IPv6 etc...}**

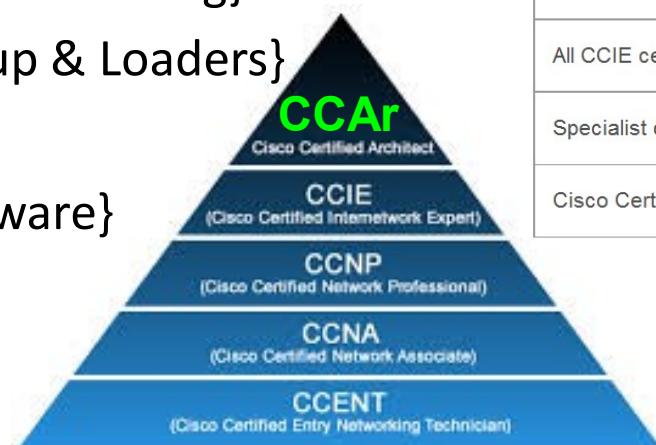
LKG **Operating System {Windows(MCSE), Linux(RHCE), VCP, MAC OS, Android & iOS}
CompTIA A+ {Hardware-Assembling & TSHOOT hardware components}**

Diploma/Degree holder – Communication Skills i.e. English {Both – Oral & Written}

Cisco Certifications

Who is Cisco?

- Founder/Inventor of Gateway i.e. Router
- Market Leader in Networking Industry i.e. IOS
- Every other vendors follows the same methodology i.e. Command Syntax
- Cisco Intensifies to hire more certified people
- Networking domains {Data Center}
 - Civil {Raised floor & False Ceiling}
 - Mechanical {Rack setup & Loaders}
 - Electrical {UPS}
 - Electronics {Hr & Software}
- Levels[5] & Tracks[8]



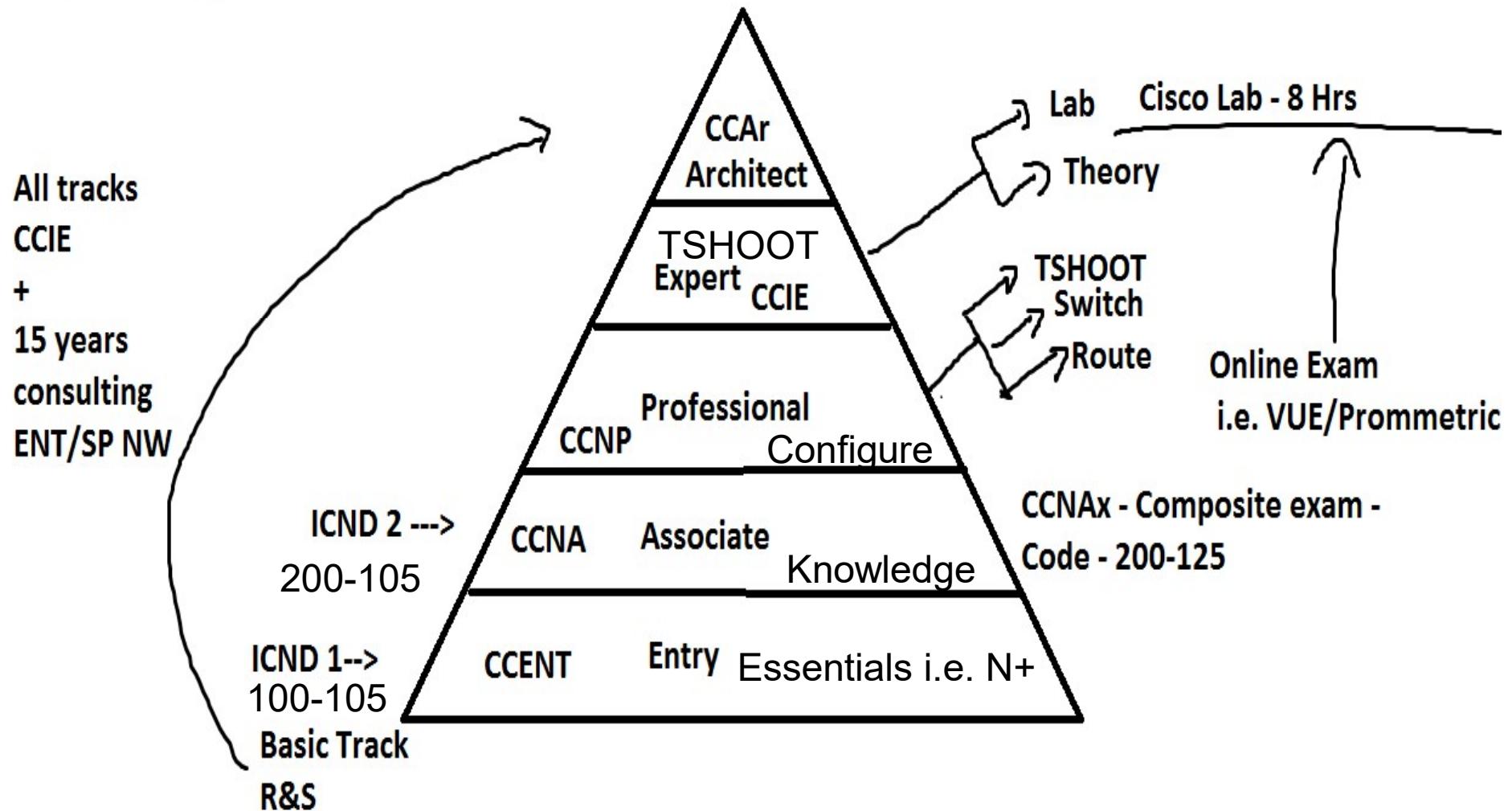
Recertification Renewal Timeframes

Certification	Duration
Entry-level, Associate-level, and Professional level	3 years
All CCIE certifications	2 years
Specialist certifications	2 years
Cisco Certified Architect	5 years

Cisco Certifications - Levels

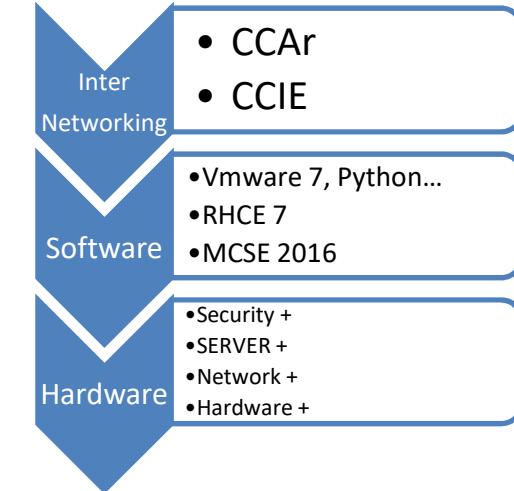
Cisco Certifications:

Levels & Tracks



Cisco Certifications - Tracks

- Basic/Core Tracks:
 1. Routing & Switching
 - Industrial
 2. Security
 - Cyber Security Operations
 3. Service Provider
 4. Wireless
- Advanced Tracks:
 5. Data Center
 6. Collaboration [IOT]
 7. Cloud [SP: AWS, Google cloud, Microsoft, VMware – IaaS, PaaS, SaaS, XaaS] - SDN
- Architect Track:
 8. Design – CCDA >>> CCDP >>> CCDE >>> 15 Years>Exp. ENT & SP NW>>> CCAr
- Other Certifications
 - Certified Technician
- Technical Specialists:
 - Collaboration, Data Center, Internet of Things, Network Programmability, Operating System Software, Security, Service Provider
- Digital Transformation Specialists:
 - Business & Customer Success



Cisco Certifications Tracks

	Entry	Associate	Professional	Expert
Architect				CCAr Architect
Cloud		CCNA Cloud	CCNP Cloud	
Collaboration		CCNA Collaboration	CCNP Collaboration	CCIE Collaboration
Cybersecurity Operations		CCNA CyberOps		
Data Center		CCNA Data Center	CCNP Data Center	CCIE Data Center
Design	CCENT	CCDA	CCDP	CCDE
Industrial / IoT		CCNA Industrial		
Routing & Switching	CCENT	CCNA Routing and Switching	CCNP Routing and Switching	CCIE Routing and Switching
Security	CCENT	CCNA Security	CCNP Security	CCIE Security
Service Provider		CCNA SP	CCNP SP	CCIE SP
Wireless	CCENT	CCNA Wireless	CCNP Wireless	CCIE Wireless
Other Certifications	Certified Technician			
Specialist	Business Security	Data Center Operating System Software	Internet of Things Service Provider	Network Programmability Collaboration

<https://learningnetwork.cisco.com/community/certifications>



IT Career paths

IT Architect

ENT NW
SP NW
15 years

Consultant:

1. Discover (Pre-Sales)
2. Design (High –level –Proposal)
3. Develop (PO – Detailed Design)
4. Deploy (Implementation)
5. Deliver (PMP -Project Management)

12. Design
ITIL, PMP, MBA

Home NW
Smart Cities
Industrial NW

WAP, WIPS,
WLAN controllers

FW, IPS, VPN
AAA,
End point SEC

9. Cyber Security Operations i.e.CEH

Vulnerability Assessment and Penetration Testing (VAPT)

7. Industrial [IOT]

5. Wi-Fi

4. Security

0. Hardware
A+, Server + & VLSI

3. Routing & Switching
NIC, Hub, Bridge, SW, Router

1. Software
OS, Apps(DB – oracle, Sql, Big data, Data warehouse, Data Mining), Programming Languages & Testing

- 1. Civil
 - 2. Mechanical
 - 3. Electrical
 - 4. Electronics
- >Computers >VT>TR>IC>MP>AI

11. Cloud [SDN]

Technologies: Virtualization, Programming
Services: IaaS, PaaS, SaaS, XaaS
Models: Private/Public/Hybrid Cloud

10. Collaboration

Voice – Ip- phone, EPABX server
Video – VC Unit
iBMS – CCTV, ACS, HVAC, PAS, FAS...

8. Data Center

Servers – (file, email, internet, apps, web....)
Storage – DAS, NAS, SAN, RAID...
LAN/WAN Load Balancer, MGT
Technologies: Virtualization, Programming

6. Service Provider

- Fiber(SONET, DWDM, CWDM)
- Frame relay, Satellite, Broadband cable
- DSL/ADSL, ISDN, ATM, PPP/multilink PPP, PPPoE
- MPLS-VPN,GSM/CDMA(LTE/4G, HSPA+,3G,Edge)
- Dialup, WiMAX, Metro Ethernet,
- Leased lines{T-1,T-3, E-1,E-3,OC3,OC12}

OPM>>>English >>> Communication skills >>> Diploma/Degree/Masters/ PhD i.e. R&D



kumar6009@gmail.com



@air.ds2

Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3

How do we train ?

- Network Diagrams, White Board Discussion, Key facts, Live Demonstrations
- Short & Palatable sessions {Both Theory & Lab}
- No Fluff, No Scripts, Just fun
- Exam Support: Dumps Review {after course }
- Dual Purpose: Knowledge & Motivation (Quiz)

Types of Learning:

Sharp [CCIE]

Troubleshooting skills



Levels of Knowledge:

3 Troubleshooting [CCIE]

Broad [CCNA]
Knowledge - Explain

2 Configure [CCNP]

Deep [CCNP]
Practice
Configuration

1 Explain [CCNA]

Destiny i.e. Wisdom
Spear of

0 Nothing



kumar6009@gmail.com



Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3

Intended Audience

This section specifies the primary and secondary target audiences of this course by job roles and notes the relevance to each job role.

- **Target candidate:**
 - Individuals seeking the Cisco CCNA® Routing and Switching certification.
 - The course is also appropriate for pre-sales and post-sales network engineers involved in the installation and support of enterprise branch office networks.
- **Key job tasks:**
 - Configure: Implement the identified solution by applying the planned implementation processes using Cisco IOS commands and applications in the correct order to the selected devices and portions of the network.
 - Verify: Use the appropriate show and debug commands and applications to ensure that the solution was correctly implemented and is performing as desired.
 - Troubleshoot: Use the appropriate show and debug commands and applications to identify the cause of basic level network issues and correctly implement a solution that ensures the network is performing as desired.
- **Job roles:**
 - Entry-level{L1} network engineer, network administrator, network support technician, or help desk technician



Pre - Requisites

- Basic computer literacy
- Basic PC operating system navigation skills
- Basic Internet usage skills
- Basic IP address knowledge
 - i.e. N+ Course – OSI Model, CIDR, VLSM, IPv6.... [20 Hrs]

Lab Requirements

- Laptop with min 4GB
- Windows Operating software i.e. win 7 or Higher version OS
- Flash/USB drive
- Notebook with Pen

Duration

- Duration { $20 \times 2\text{Hrs} = 40\text{ Hrs}$ } { Monday to Friday – Thursday is holiday}
- Cisco = 40 Hrs



200-125 - CONTENTS AT A GLANCE

1. Network Fundamentals{15%}

OSI & TCP/IP Models, TCP & UDP Protocols, Infra components{Firewall, Access points, Wireless controllers}, Cloud {Internal & External cloud services, Virtual services, Virtual NW Infra}, Collapsed core & three-tier arch, Topologies {Star, Mesh, Hybrid}, Cabling, TSHOOT methodologies, IPV4 addressing & Subnetting, Ipv6 (Auto & Stateless Config), IPv6 address types {Global unicast, Unique local, Link Local, Multicast, modified EUI-64, Anycast}

2. LAN Switching Technologies {21%}

Concepts {Mac learning & aging, Frame switching, Frame flooding, MAC address table}, Ethernet frame format, TSHOOT {collisions, errors, duplex, speed}, VLANS{Normal/extended range, access ports –data/voice,}, Interswitch connectivity {Trunk, Pruning, DTP, VTP {v1 & v2} & 802.1Q, Native VLAN}, STP {mode {PVST+, RPVST+} & root bridge selection}, STP features {Port fast, BPDU guard}, Layer 2 protocols{CDP & LLDP}, Etherchannel {Layer2/Layer3 – static, PAGP & LACP}, Switching Stacking & Chassis aggregation

3. IP Routing Technologies {23%}

Concepts {Route Lookup & Frame rewrite}, Route Table {prefix, network mask, next hop, routing protocol code, administrative distance, metric, Gateway of last resort}, Inter-VLAN routing {Routing on stick & SVI}, Routing Types { Static & Dynamic}, Routing Protocols {Distance vector, Link State, Interior & Exterior}, Static routing { Default route, network route, Host route, Floating Static}, RIPv2{IPV4}, OSPFv2 Single area & Multi area {IPv4 & IPv6}, EIGRP {IPv4 & IPv6}, TSHOOT

4. WAN Technologies {10%}

PPP & MLPPP{Local Auth}, PPPOE client side {local auth}, GRE tunnel, WAN {point-to-point, Hub & spoke, Full mesh, single vs dual-homed}, WAN connectivity options {MPLS, Metro Ethernet, broadband PPPOE, Internet VPN {DMVPN, Site-to-Site VPN, Client VPN}, eBGP {Single-homed – peering, route advertising using network command only}, QOS concepts {marking, device trust, Prioritization {voice, video & data}, shaping, policing, congestion management}}

5. Infrastructure Services {10%}

DNS lookup, TSHOOT {DNS Client}, DHCP {server, Relay, Client, TFTP, DNS & gateway options}, TSHOOT{DHCP}, HSRP {Priority, preemption, version}, NAT {Static, pool & PAT}, NTP {Client/Server}

6. Infrastructure Security {10%}

Port Security { static, Dynamic, Sticky, max mac add, violation actions, Err-disable recovery}, Common access layer threat mitigation {802.1x, DHCP snooping, Non default Native VLAN}, IPv4 & IPv6 ACL {Standard, Extended, Named}, APIC-EM path trace ACL analysis tool, Basic device hardening {local auth, Secure Password, Access to device {Source add, Telnet/SSH}, Login banner}, Device security using AAA {TACACS+ & RADIUS}

7. Infrastructure Management {10%}

Device monitoring protocols {SNMPv2, SNMPv3, syslog}, TSHOOT {issues using ICMP echo-based IP SLA}, Device MGT {Backup & Restore device config, CDP, LLDP, Licensing, Logging, Time zone , Loopback}, Intial device config, Device maintenance {Cisco IOS upgrades & recovery {SCP, FTP, TFTP & MD5 verify} , Password recovery & configuration register , File system management} IOS troubleshoot tools {ping & trace route with extended option, terminal monitor, log events, localSPAN}, Network programmability {controller, control & data plane, Northbound & south bound API's}

<https://learningnetwork.cisco.com/community/certifications/ccna/ccna-exam/exam-topics>



kumar6009@gmail.com



@air.ds2

Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3

25

Course Outline {CCNA R&S – 20x2=40Hrs}

Class 01: Topics: Introduction: Name, Education, IT experience Syllabus, Lab Details, Duration Network Fundamentals: 1. OSI & TCP/IP Model	Class 06: Topics: LAN Switching Technologies: 1. NW devices & BD/CD 2. IOS, Telnet, SSH, MGT IP	Class 11: Topics: Routing Technologies: 1. NW, Host, Default, RIP, Floating route]	Class 16: Topics: Infrastructure Services: 1. ACL, NAT, 2. NTP, DNS, DHCP, 3. HSRP,
Class 02: Topics: Network Fundamentals: 1. OSI & TCP/IP Model 2. Bin> dec/Hexa Conversions 3. MAC address	Class 07: Topics: LAN Switching Technologies: 1. VLAN, Trunk & VTP	Class 12: Topics: Routing Technologies: 1. EIGRP	Class 17: Topics: WAN Technologies: 1. Basics 2. PPP, MLPP, PPPoE
Class 03: Topics: Network Fundamentals: 1. Enterprise NW infrastructure 2. Topology, cables & connectors 3. TSHOOT Approach & Methods	Class 08: Topics: Switching Technologies: 1. STP, PVSTP, RSTP	Class 13: Topics: Routing Technologies: 1. OSPF [Single Area]	Class 18: Topics: WAN Technologies: 1. VPN - GRE tunnel 2. eBGP 3. QOS
Class 04: Topics: Network Fundamentals: 1. IPv4 Basics 2. CIDR to Subnet mask conversion	Class 09: Topics: Switching Technologies: 1. Ether channel 2. Inter-VLAN Routing 3. GNS3 + Real Lab	Class 14: Topics: Routing Technologies: 1. OSPF {Multiple area}	Class 19: Topics: Infrastructure Security: 1. Terminologies, AAA 2. SW port Sec
Class 05: Topics: Network Fundamentals: 1. Class C Subnetting, VLSM 2. IPv6 Basics	Class 10: Topics: Routing Technologies: 1. Routing Basics 2. Serial [WAN] 3. Interpret NW diagram	Class 15: Topics: Routing Technologies: 1. IPv6 – static, ospf, eigrp	Class 20: Topics: Infrastructure Management: 1. Licensing, rou psswd rec 2. NW Programming



Course Outline – Fast Track {CCNA R&S – 8x5=40Hrs}

Day 1[Tuesday]	Day 2[Wednesday]	Day 3[Thursday]	Day 4[Friday]	Day 5[Monday]
Time: 9am to 1pm Topics: Foundations 1. Introduction 2. OSI & TCP/IP Model	Time: 9am to 1pm Topics: Switching 1. Lines, Block {PT} 2. Modes & Show 3. Cisco Packet Tracer	Time: 9am to 1pm Topics: Routing 1. Basics 2. Static/Dynamic Routing	Time: 9am to 1pm Topics: IP Services 1. ACL, 2. NAT, 3. DNS,	Time: 9am to 1pm Topics: INFRA SEC 1. Terminologies 2. AAA
Tea Break: 10:30am to 10:45am	Tea Break: 10:30am to 10:45am	Tea Break: 10:30am to 10:45am	Tea Break: 10:30am to 10:45am	Tea Break: 10:30am to 10:45am
3. ENT NW INFRA 4. Topology & Media 5. TSHOOT Approach & methods	3. IOS Basics 4. Telnet 5. SSH 6. SW MGT IP	3. NW route, 4. Host route, 5. Default route,	DHCP{GNS3} 4. HSRP, 5. NTP	3. Switch port Security 4. APIC-EM ACL path trace tool
Time: 1pm to 1:30pm Lunch	Time: 1pm to 1:30pm Lunch	Time: 1pm to 1:30pm Lunch	Time: 1pm to 1:30pm Lunch	Time: 1pm to 1:30pm Lunch
Time:1:30pm to 6pm Topics: Foundations 6. BIN >Dec/Hexa Conversion 7. IPv4 Basics	Time:1:30pm to 6pm Topics: Switching 7. VLAN, Trunk, VTP 8. STP, PVSTP, RSTP	Time:1:30pm to 6pm Topics: Routing 6. RIPv2, 7. Floating route 8. EIGRP	Time:1:30pm to 6pm Topics: WAN 1. Basics 2. HDLC, PPP {CHAP, PPPoE, MLPPP}	Time:1:30pm to 6pm Topics: INFRA MGT 1. SNMP, SYSLOG 2. Licensing 3. ROU PSSWD recovery
Tea Break: 3:30pm to 3:45pm	Tea Break: 3:30pm to 3:45pm	Tea Break: 3:30pm to 3:45pm	Tea Break: 3:30pm to 3:45pm	Tea Break: 3:30pm to 3:45pm
8. Class C Subnetting 9. VLSM, 10. IPv6 Basics	9. L2/L3 Etherchannel 10. Inter-VLAN Routing 1. Router on stick 2. L3 Switching	9. OSPF Single Area 10. OSPF Multi-Area	3. QoS 4. VPN {GRE}} 5. eBGP	4. TFTP 5. Terminal Monitor 6. Network Programming



How to get the most from this Course:

- Repetition, Repetition, Repetition
- Take notes, Write down all Key Information you hear
- **How to Build a Lab?**
 - Simulator - Cisco Packet Tracer {CCNA} - 90% Lab
 - Emulator{Virtual Router} – GNS 3 {min 4GB ram} {CCNP/CCIE} – 10% Lab
 - Real Labs – CCNA/CCNP/CCIE Rack [Putty]
 - CCNA {R&S} = 3 Router, 1L3 Switch, 1 L2 Switch & 1 Access server
 - CCNP /CCIE {R&S}= 6 Routers, 2 L3 switches & 2 L2 Switches & 1 Access server
- Study Hard {Understand the Concepts}
- Dig Deeper
 - {No Politics & Only Practice – My life is my message – Mahatma Gandhi}
- No mobiles chatting in class hours
 - You will know; What you LOVE. That's all !!!

“WELCOME TO THE WORLD OF CISCO”



Questions & Answers (Max-15 Mins)



Network Fundamentals

OSI & TCP/IP Models

Lesson 5

Binary Units:

0 or 1	= 1bit
8 bits	= 1Byte
1024 Bytes	= 1KB
1024 KB	= 1MB
1024 MB	= 1GB
1024 GB	= 1TB
1024 TB	= 1PB

Table 1: Data Measurement Units

Unit	Abbreviation	Decimal Value	Binary Value	Decimal Size
bit	b	0 or 1	0 or 1	1/8 of a byte
byte	B	8 bits	8 bits	1 byte
kilobyte	KB	$1,000^1$ bytes	$1,024^1$ bytes	1,000 bytes
megabyte	MB	$1,000^2$ bytes	$1,024^2$ bytes	1,000,000 bytes
gigabyte	GB	$1,000^3$ bytes	$1,024^3$ bytes	1,000,000,000 bytes
terabyte	TB	$1,000^4$ bytes	$1,024^4$ bytes	1,000,000,000,000 bytes
petabyte	PB	$1,000^5$ bytes	$1,024^5$ bytes	1,000,000,000,000,000 bytes
exabyte	EB	$1,000^6$ bytes	$1,024^6$ bytes	1,000,000,000,000,000,000 bytes
zettabyte	ZB	$1,000^7$ bytes	$1,024^7$ bytes	1,000,000,000,000,000,000,000 bytes
yottabyte	YB	$1,000^8$ bytes	$1,024^8$ bytes	1,000,000,000,000,000,000,000,000 bytes



OSI and TCP/IP models

- Open systems/Source Interconnection i.e. OSI
 - Developed by International organization for Standardization {ISO}
 - Blue Print
 - Starting a Company Example i.e. Departments{Layers}, Procedures{Protocols} etc..
 - For Hardware, Networking & Software Developers
- TCP/IP Model
 - Transmission Control Protocol/Internet Protocol
 - TCP/IP is also a Protocol Suite
- Layered approach:
 - Long network communication process divided into smaller & simpler pieces. So it is easy for design, development & Trouble shooting
- Advantages :
 - Allow multiple vendors development through standardization of Network Components
 - Industry standardization defines what functions occurs at each layer
 - Allows various types of network devices & software to intercommunicate
 - It prevents changes in one layer from affecting other layers.
 - **So it does not hamper the Research & Development**

OSI model – Upper Layer functions

- Layer 7
 - Application Layer
 - It provides user interface i.e. OS, Applications [HTTP, DNS, DHCP]
- Layer 6
 - Presentation Layer
 - It provides international standard formats
 - > Word[.docx, .xlsx, .pdf]; Picture[.bmp, .jpeg]; Audio[.mp3, .wav]; Video[.mp4, .flv]
 - It performs data compression (.zip & .rar) & data encryption (3DES/RSA)
- Layer 5
 - Session Layer
 - It establish {start}, maintain & end sessions (SCP/NetBios)
 - It keep the data separate for each application
 - By different source port no.

OSI model – Lower Layer functions

- Layer 4
 - Transport Layer {Middle Manager}
 - It provides Connection-oriented reliable{TCP} & Connection-less unreliable{UDP} communication
 - It performs error correction, before retransmission
- Layer 3 Devices : Router
 - Network Layer
 - It provides logical addressing i.e. Routed Protocols
 - IPv4 & IPv6{cisco & Microsoft}
 - IPX – Internet Packet Exchange {Novell}
 - AppleTalk – {Macintosh}
 - It performs path determination i.e. Routing Protocols– RIP, EIGRP, OSPF & BGP
- Layer 2 Devices : Bridges & Switches
 - Data-link Layer
 - LLC Layer {Logical Link Control}
 - It combines packets to bytes & bytes to frame
 - MAC Layer {Media Access Control}
 - It provides access to media through physical address {Protocol: LAN-Ethernet-MAC address}
 - It performs data error detection, not correction
- Layer 1 Devices : Repeaters & Hubs
 - Physical Layer
 - Moves bits between hosts
 - It provide international standards for voltage, wire speed, cable {UTP}& connectors [RJ45]....



Commonly used TCP and UDP default ports

• TCP ports

- FTP – 20, 21
- SSH – 22
- TELNET – 23
- SMTP – 25
- DNS – 53
- HTTP – 80
- POP3 – 110
- IMAP4 – 143 {Internet Mail Access Protocol}
- HTTPS – 443

What is a port number?

Logical Interface for Applications [L7 Protocols]

IANA {Internet Assigned Numbers Authority}

- Range 0 – 65,535
- Three Blocks
 - Well known ports 0 - 1023
 - Registered ports: 1025 – 49,151
 - Dynamic or Private ports: 49,152 – 65,535

• UDP ports

- TFTP – 69 (IOS Image & Device Configuration Backup(storage))
- NTP – 123 (Time Sync of devices)
- DNS – 53
- BOOTPS/DHCP – 67 (Automatic configure IP, SM, DG, Domain Name & Leased Period)
- SNMP – 161 (Grabs Statistics{i.e. CPU & RAM %} from Devices)

• To verify:

- PC - CMD> netstat

<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>



kumar6009@gmail.com



@air.ds2

Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3

34

Commonly used TCP and UDP default ports

TCP : Connection-oriented{Session} & Reliable{ACK} Communication

S/N	Application	Function	L4 Protocol	L7 Protocol	Port No/Add:	Full Name
1	WIN 7	Data Transfer	TCP	FTP	20 = Data Plane 21 = Control Plane	File Transfer Protocol
2	Putty	Remote Login - Plain Text COM.	TCP	Telnet	23	Telecommunication Network
3	Putty	Remote Login - Cyper Text COM.	TCP	SSH	22	Secure Shell
4	Chrome	Web Browsing - Plain Text COM.	TCP	HTTP	80	Hyper Text Transfer Protocol
5	Firefox	Web Browsing - Cyper Text COM.	TCP	HTTPS	443	Hyper Text Transfer Protocol - Secured
6	outlook	Dowload mails from internet mail box to local Mail box i.e. Cut & Paste	TCP	POP3	110	Post Office Protocol version 3
7	outlook	Dowload mails from internet mail box to local Mail box i.e. Copy & Paste	TCP	IMAP4	143	Internet Mail Access Protocol version 4
8	outlook	Send/Receive Emails	TCP	SMTP	25	Simple Mail Transfer Protocol
9	WIN2016	Resolution : FQDN > IP address	TCP	DNS	53	Domain Name Service

**UDP : Connection-less{No Session} & Unreliable{No ACK} Communication
i.e. real time apps {voice, video, online games}**

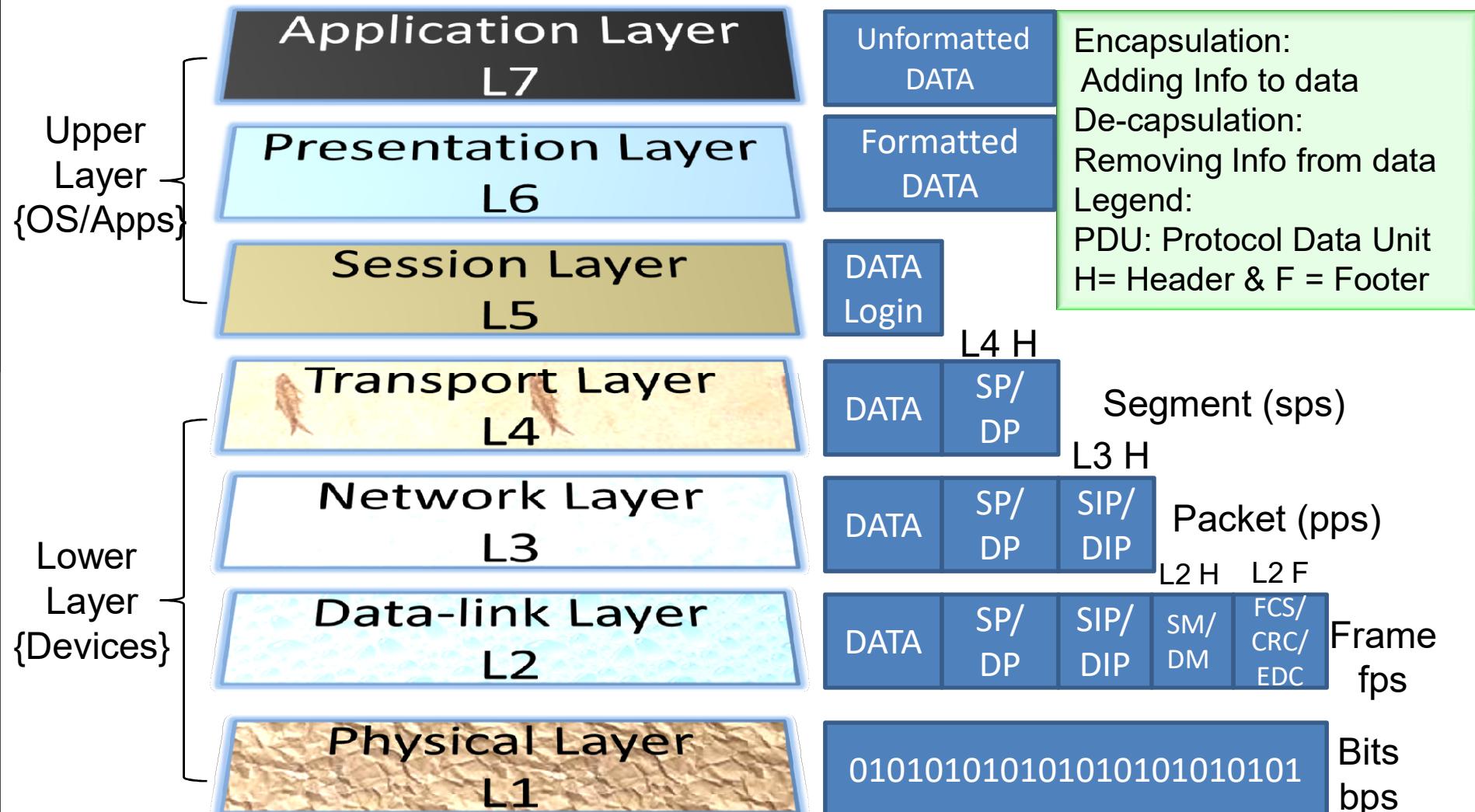
S/N	Application	Function	L4 Protocol	L7 Protocol	Port No/Add:	Full Name
1	Cisco TFTP	IOS Image & Device Configuration Backup	UDP	TFTP	69	Trival File Transfer Protocol
2	WIN2016	SYNC Time Btween all Network devices	UDP	NTP	123	Network Time Protocol
3	WIN2016	Resolution : FQDN > IP address	UDP	DNS	53	Domain Name Service
4	WIN2016	OS booting with user involvement	UDP	BOOTP	67	Bootstrap Protocol
5	WIN2016	Automatically configuring IP Add...	UDP	DHCP	67	Dynamic Host Configuration Protocol
6	HP openview	Grab Device Statistics i.e. CPU & RAM %	UDP	SNMP	161	Simple Network Management Protocol

Workflow: User >>> Applications >>> L7 Protocols > L4 Protocols > port no >Server



OSI model

Data Encapsulation



Legend: FCS = Frame Checking Sequence; CRC: Cyclic Redundancy Check; EDC: Error Detection Code

Open Systems Interconnection(OSI) model

Common Protocols

OSI MODEL

TCP/IP Protocol suite

All follow i.e.
Software & Hardware
Vendors worldwide



TCP:FTP, SSH, Telnet, SMTP, DNS, HTTP, POP, IMAP4, HTTPS
UDP: TFTP, NTP, DNS, BOOTPS/DHCP, SNMP

Text:.. pdf, .xls, .docx, Image: .jpeg, .gif, .png,
compression: .zip, .rar; encryption:3DES, RSA

SCP, Netbios

TCP, UDP

Routed Protocol: IPv4, IPv6, IPX, Appletalk
Routing Protocol: RIP, EIGRP, OSPF, BGP

LAN: Ethernet(e0, Fe0/0,Giga 0/0), Token Ring, FDDI
WAN:HDLC, PPP, PPPoE, Frame Relay, ATM, MPLS

LAN: RG58, RG9, UTP -CAT5, CAT5e, CAT6, RJ45, RJ11
WAN: DCE/DTE serial cable, V.35, E1, T1, E3, T3, Y1

Numbering systems-Conversions

Numbering systems

- Binary {0 & 1} - Computer Machine understand only 0's & 1's
- Octal {0–7}
- Decimal {0-9}
 - port No{16 bits}, IPv4{32 bits} – dotted Decimal Notation
- Hexa-decimal {0-9, A{10}, B{11}, C{12}, D{13}, E{14} & F{15}}
 - >MAC address {48 bits} – 12 hexa digits & IPv6 Address {128 bits}- 32 digits

• Conversions

- Binary octet[8 bits] to Decimal Conversion

128	64	32	16	8	4	2	1
0	1	1	0	1	0	0	1
0 +	64 +	32 +	0 +	8 +	0 +	0 +	1 = 105

- Decimal to Binary octet Conversion

- 1, 255, 121, 63, 127, 240, 252, 3, 130, 10

- Binary to Hexa Decimal Conversion i.e. 1 Hexa digit = 4 bits

- Hexa-Decimal digits to Binary bits Conversion

- 0123:4567:89AB:CDEF



OSI and TCP/IP models

Network Layer Protocol: IP version 4

Class	Subnet Mask decimal	No. of Hosts per Network	No. of Networks	Start -End Address	
A	255.0.0.0	16 Million	127	1.0.0.0 - 126.255.255.255	N.H.H.H
B	255.255.0.0	65000	16000	128.0.0.0 - 191.255.255.255	N.N.H.H
C	255.255.255.0	254	2 Million	192.0.0.0 - 223.255.255.255	N.N.N.H
D	Reserved for multicast groups			224.0.0.0 - 239.255.255.255	
E	Reserved for future use, or Research and Development Purposes			240.0.0.0 - 254.255.255.254	

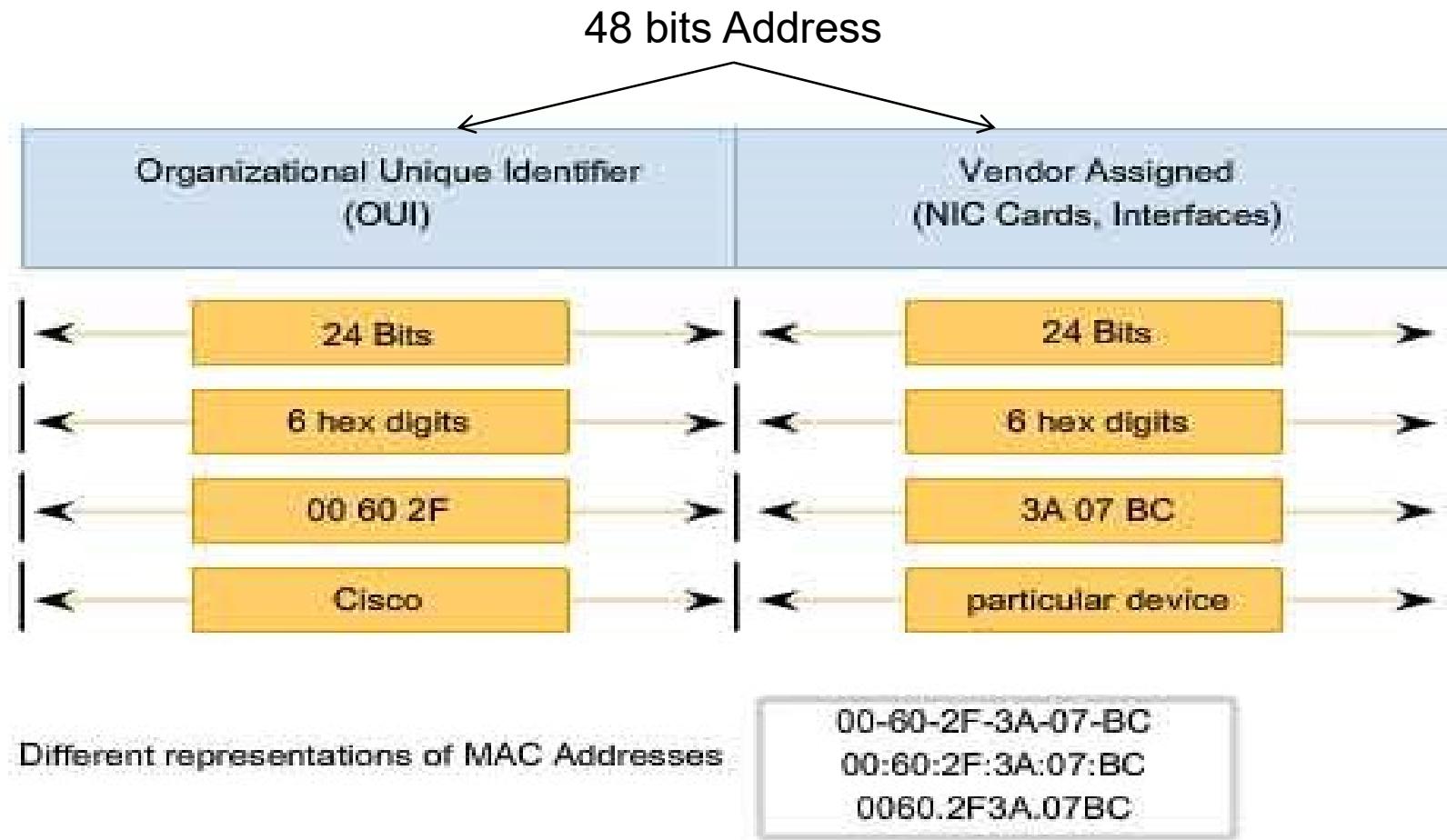
Private IP Address Range:

Class	Address Range	Default Subnet Mask
A	10.0.0.0 - 10.255.255.255	255.0.0.0
B	172.16.0.0 - 172.31.255.255	255.255.0.0
C	192.168.0.0 – 192.168.255.255	255.255.255.0



OSI and TCP/IP models

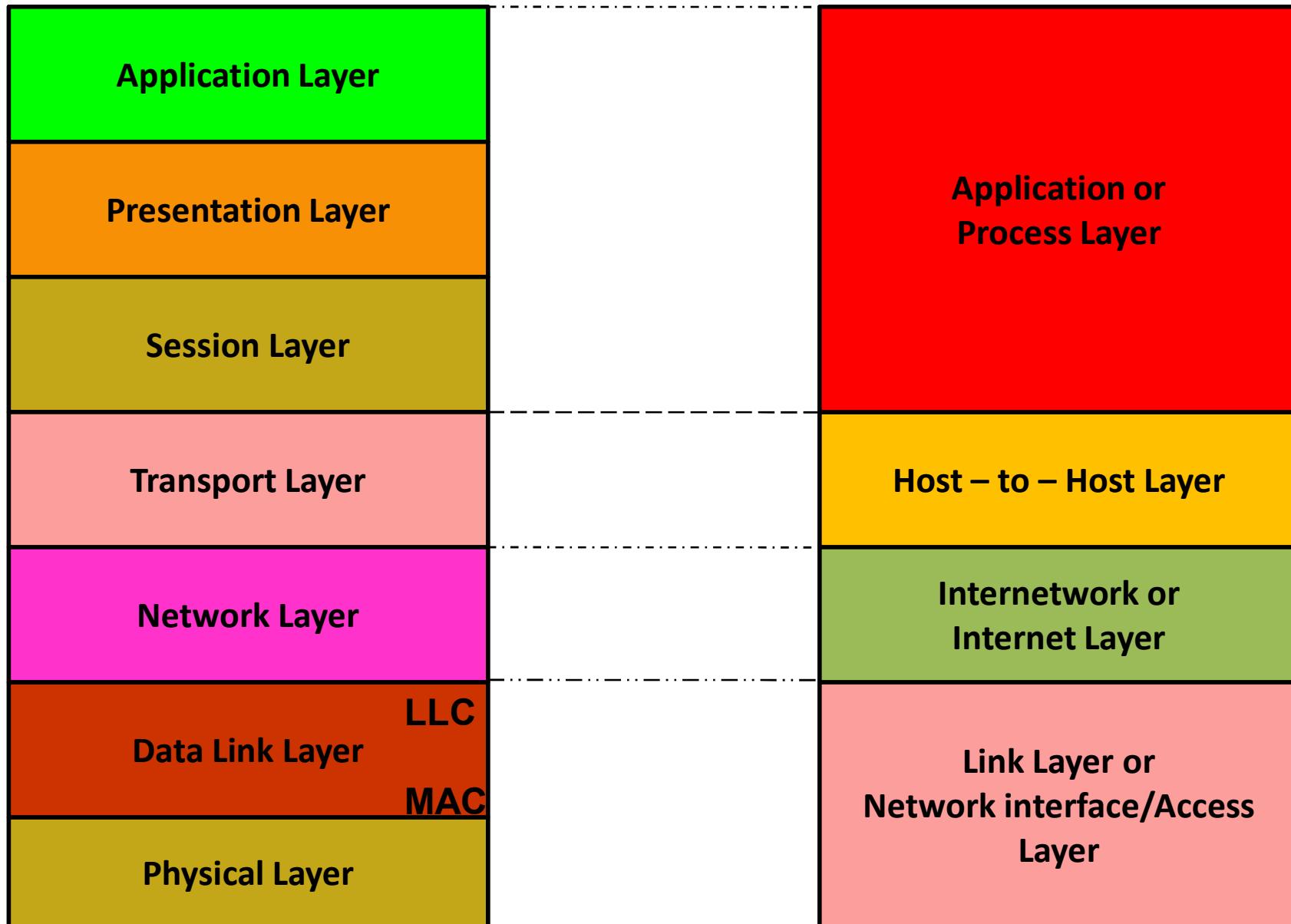
Media Access Control {MAC} Address



<http://standards-oui.ieee.org/oui.txt>



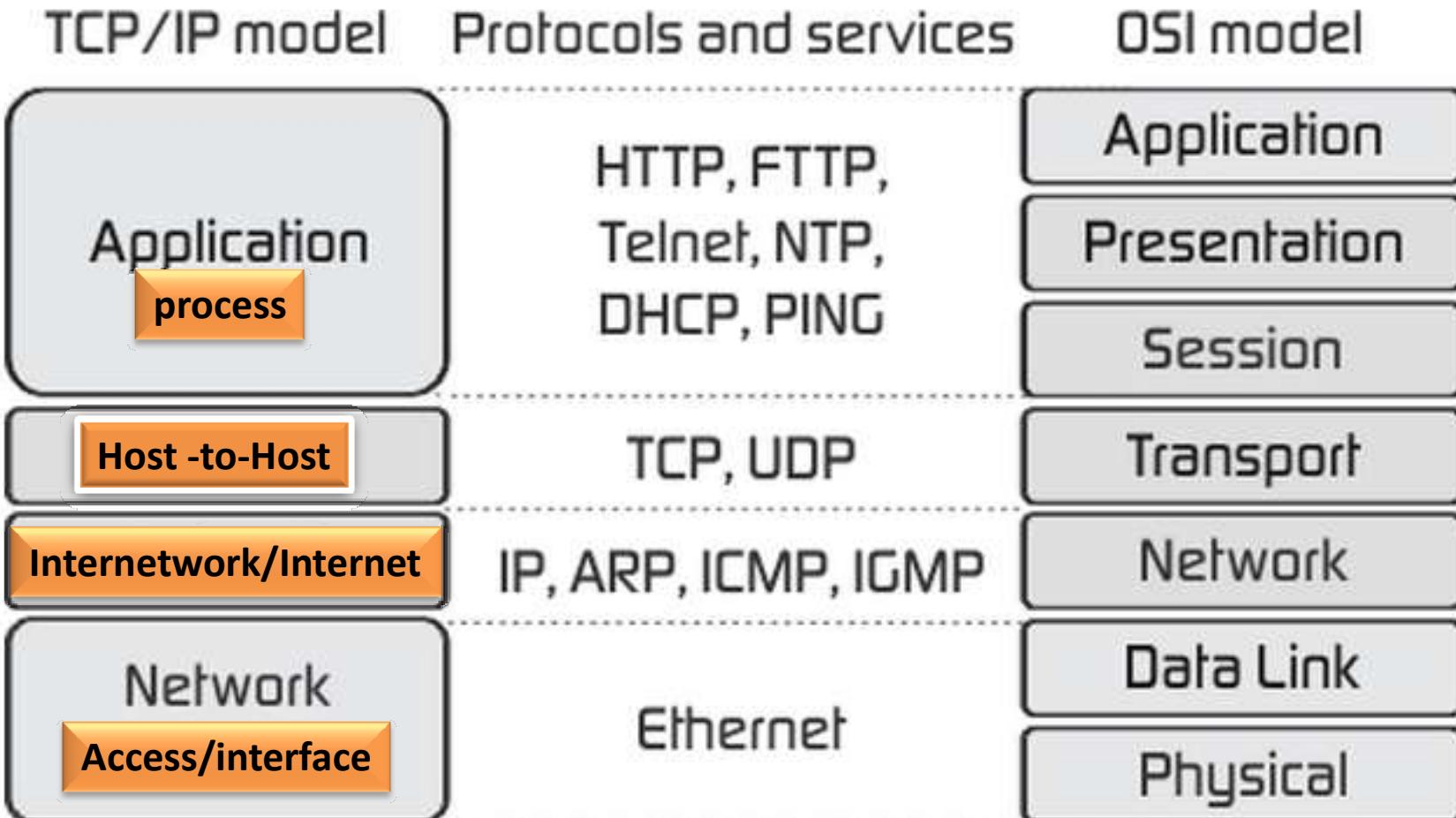
OSI model vs. TCP/IP Model



OSI and TCP/IP models

OSI Model vs. TCP/IP Model

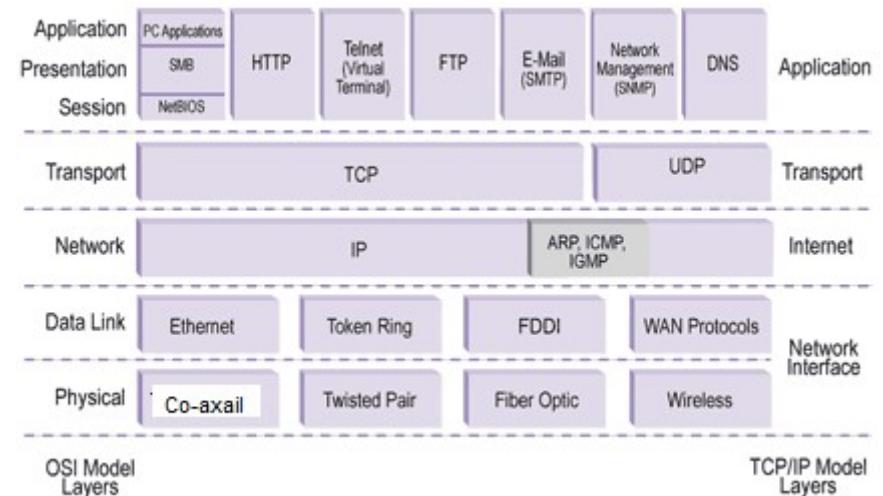
DOD/Host-to-Host/



Network Fundamentals

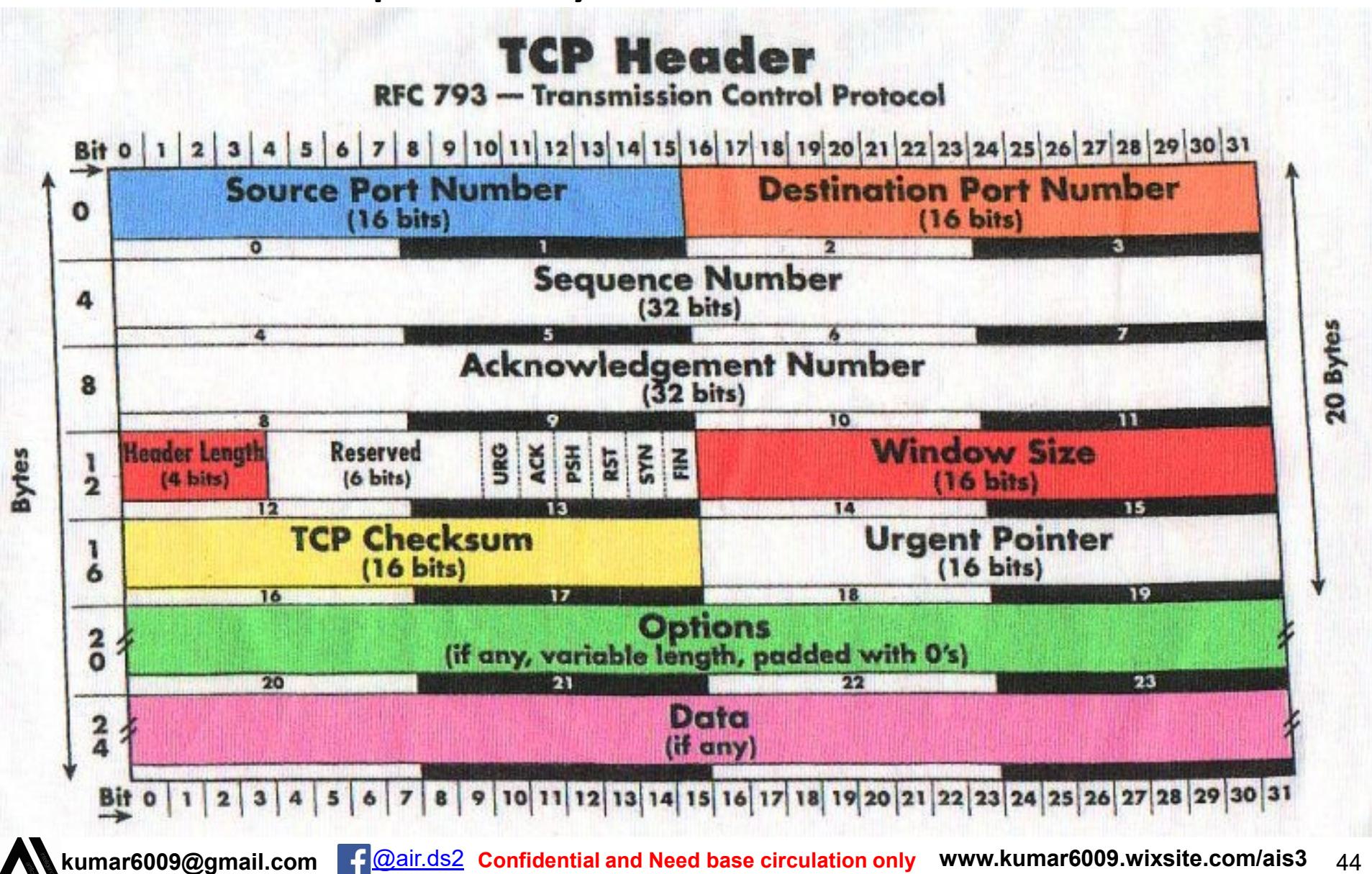
TCP/IP Protocols suite

Lesson 5

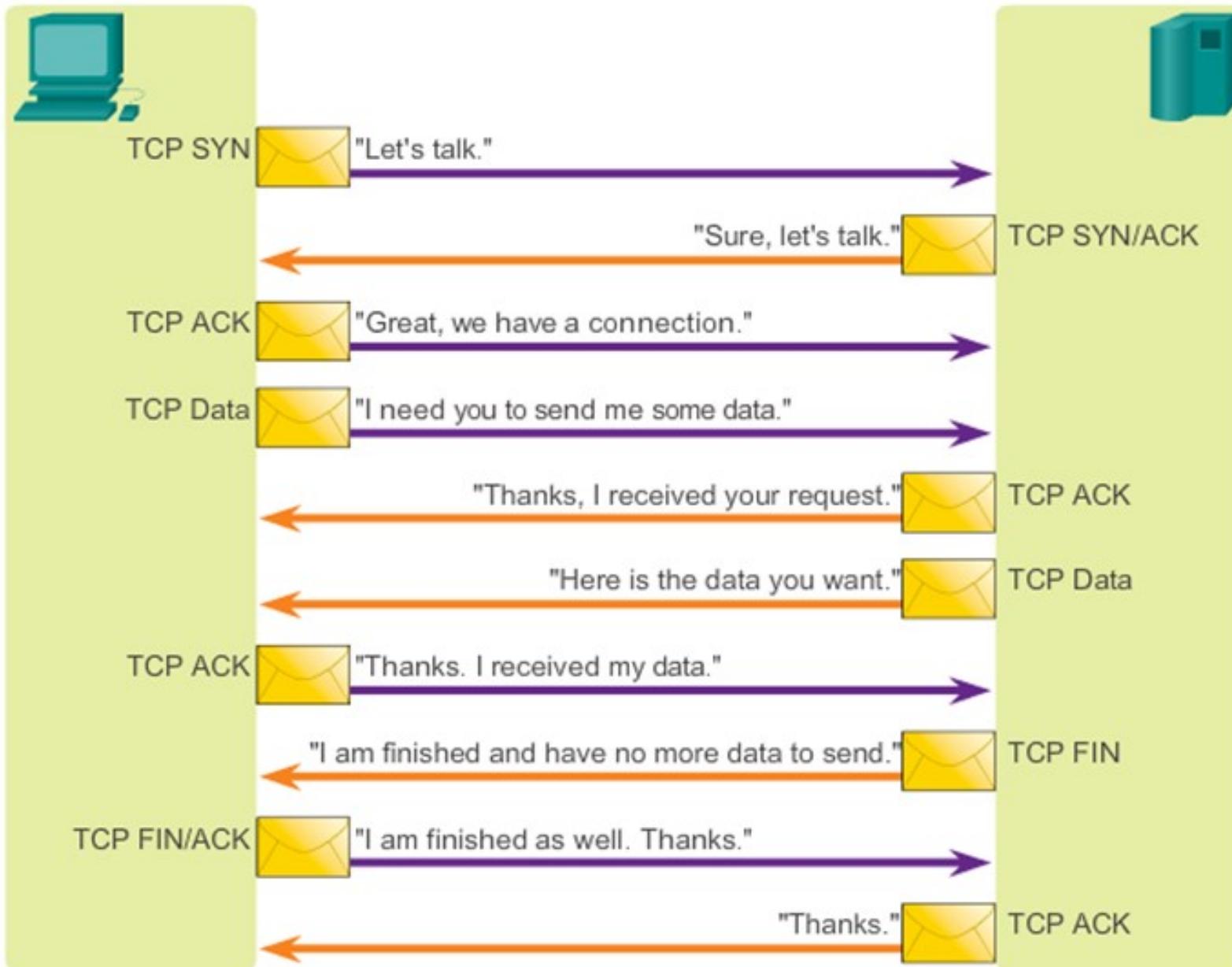


TCP/IP Protocols

L4 - Transport Layer Protocol: TCP Header



TCP Conversation



OSI model

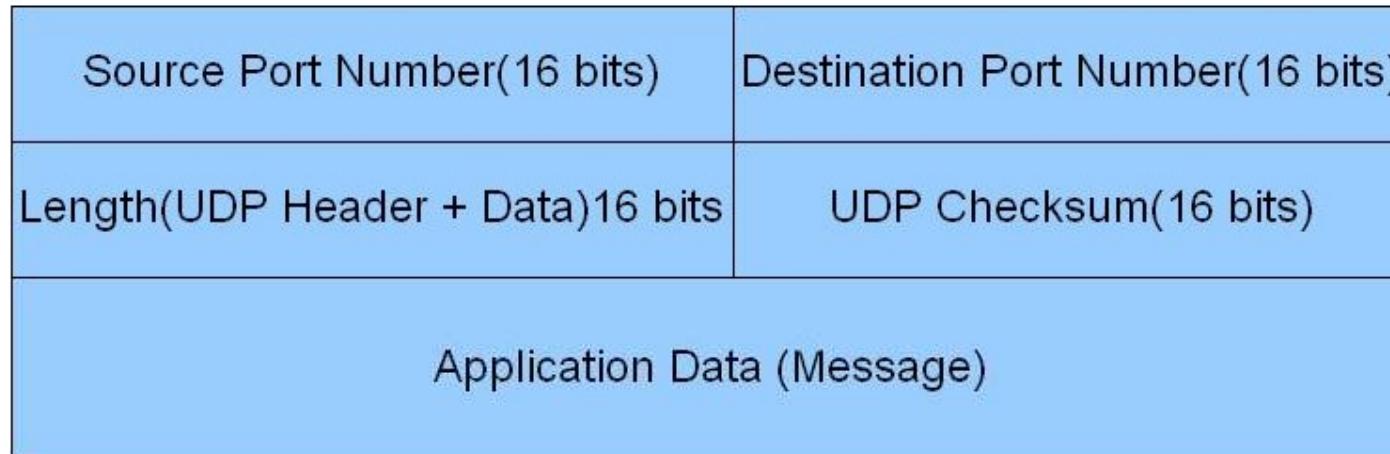
Transport Layer Protocol: UDP Header

User Datagram Protocol

0

15 16

31



8
Bytes

Network MTU	(bytes)
1. 16 Mbps Token Ring	17914
2. 4 Mbps Token Ring	4464
3. FDDI	4352
4. Ethernet	1500
5. IEEE 802.3/802.2	1492
6. PPPoE (WAN Miniport)	1480
7. X.25	576



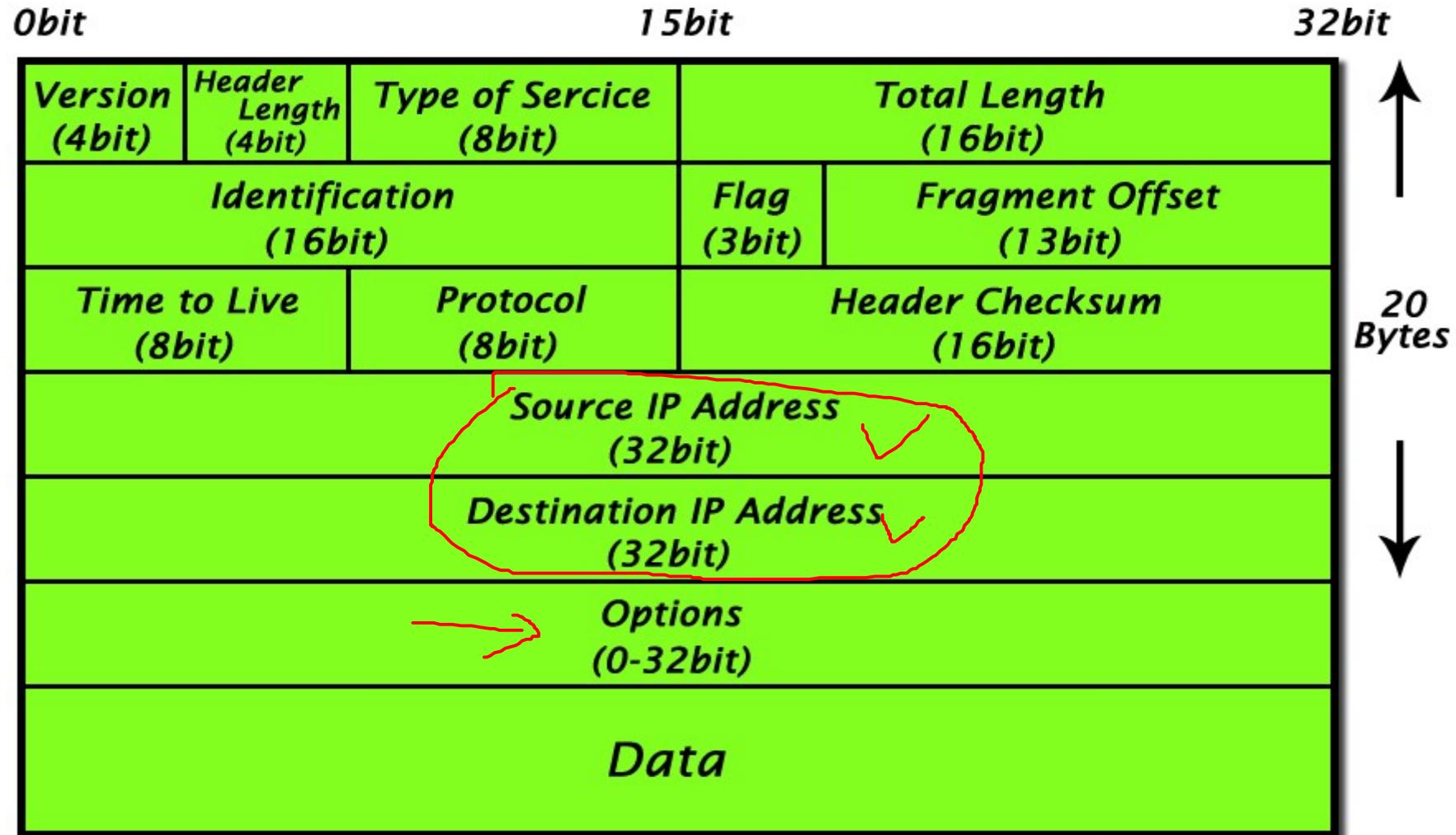
OSI and TCP/IP models

TCP vs. UDP

TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement

TCP/IP Protocols

L3 - Network Layer Protocol: IPv4 Header



L4 Layer Services (protocols)	Protocol Number
Internet Control Message Protocol (ICMP) (Ping)	1
Transmission Control Protocol (TCP)	6
User Datagram Protocol (UDP)	17
General Routing Encapsulation (PPTP data over GRE)	47
Authentication Header (AH) IPSec	51
Encapsulation Security Payload (ESP) IPSec	50
Exterior Gateway Protocol (EGP)	8
Gateway-Gateway Protocol (GGP)	3
Host Monitoring Protocol (HMP)	20
Internet Group Management Protocol (IGMP)	88
MIT Remote Virtual Disk (RVD)	66
OSPF Open Shortest Path First	89
PARC Universal Packet Protocol (PUP)	12
Reliable Datagram Protocol (RDP) (EIGRP)	27
Reservation Protocol (RSVP) QoS	46



TCP/IP Protocols

L3 - Network Layer Protocol: IPv6 Header



IPv4 vs. IPv6

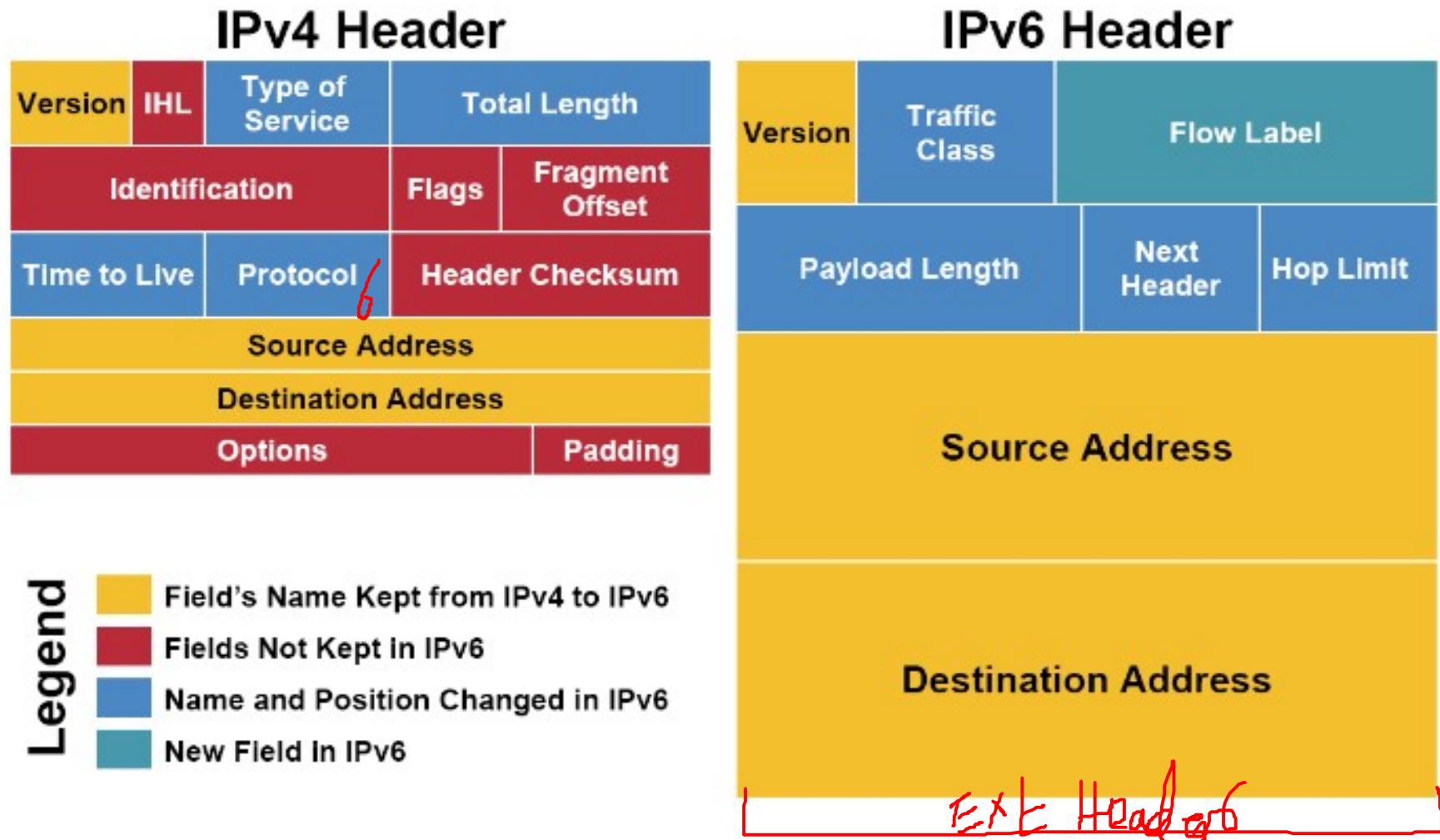


FIG. 1. IPv4 header and IPv6 header [5]

TCP/IP Protocols

L2 – Data Link layer : Ethernet Header

Preamble	Destination	Source	Type	Data		CRC
----------	-------------	--------	------	------	--	-----

ETHERNET II (DIX)

Preamble	Destination	Source	Length	Protocol	Data	CRC
----------	-------------	--------	--------	----------	------	-----

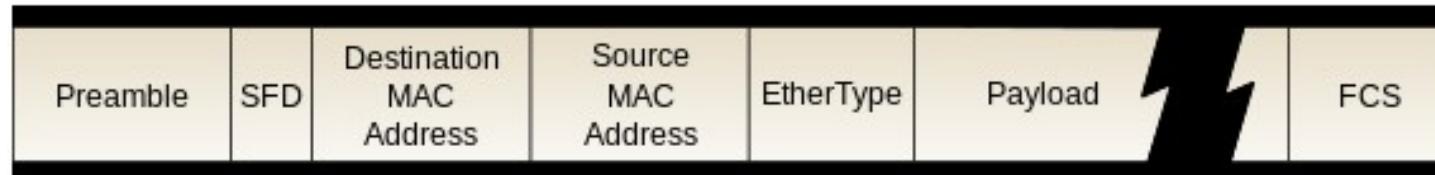
IEEE 802.3 "Raw" (No LLC) (Netware's 802.3)

Preamble	Destination	Source	Length	LLC Standard	Data	CRC
----------	-------------	--------	--------	--------------	------	-----

IEEE 802.3 Standard

Preamble	Destination	Source	Length	LLC SNAP	Data	CRC
----------	-------------	--------	--------	----------	------	-----

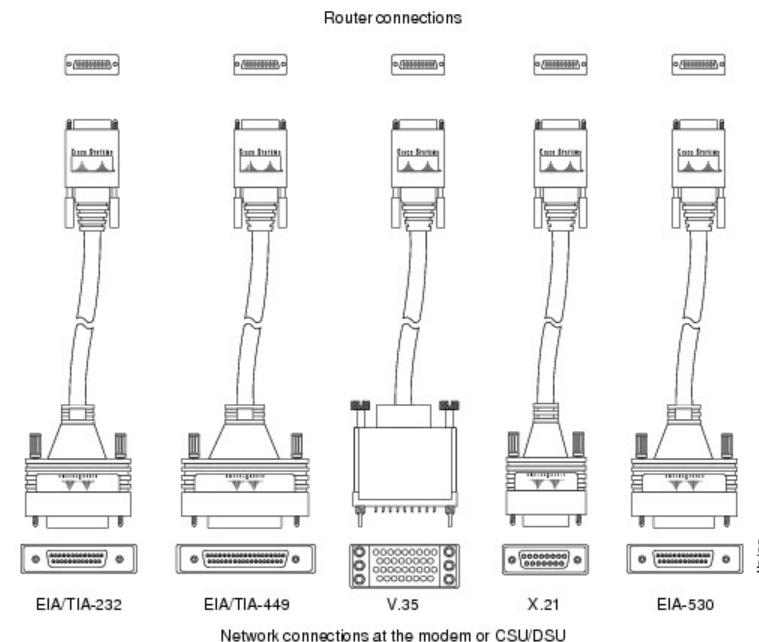
IEEE 802.3 SNAP



TCP/IP Protocols

L1 – Physical layer : Cables & Connectors

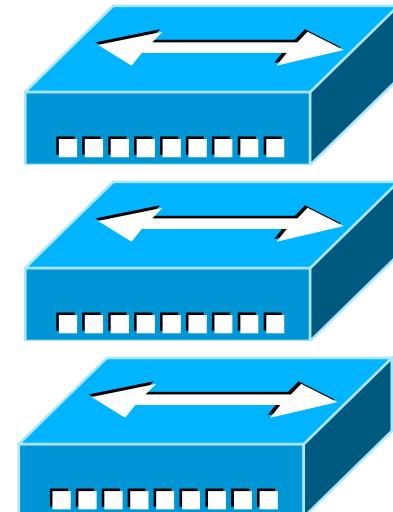
- LAN
 - Cables & Connectors
 - Co-axial(Thin net & Thick net) & RG58, RG9,
 - Twister-pair(STP, UTP – CAT5e, CAT6, CAT7) & RJ45, RJ11,
 - Fiber (MMF & SMF) & ST, SC, ST, MPO
- WAN
 - Cables
 - Serial Cables/DCE or DTE cables
 - Connectors
 - V.35 connector



Network Fundamentals

Enterprise Network Infrastructure Design

Lesson 2



Enterprise Network Infrastructure

➤ Types of Networks:

1. Peer to Peer NW - Btwn. PC's
2. LAN - Single Building
3. CAN - Campus
4. MAN - Within a City
5. WAN - Inter city/State/Country/Planet/Universe
 1. Intranet - Private - Same Org.
 2. Extranet - Private - Diff. Org.
 3. Internet - Public WAN
 4. PSTN Cloud - Public Switched Telephone NW
 5. DC Cloud - services i.e. storage, email & web server
 1. Private cloud
 2. Public cloud
 3. Hybrid Cloud
 4. Community Cloud

➤ Class Of Networks:

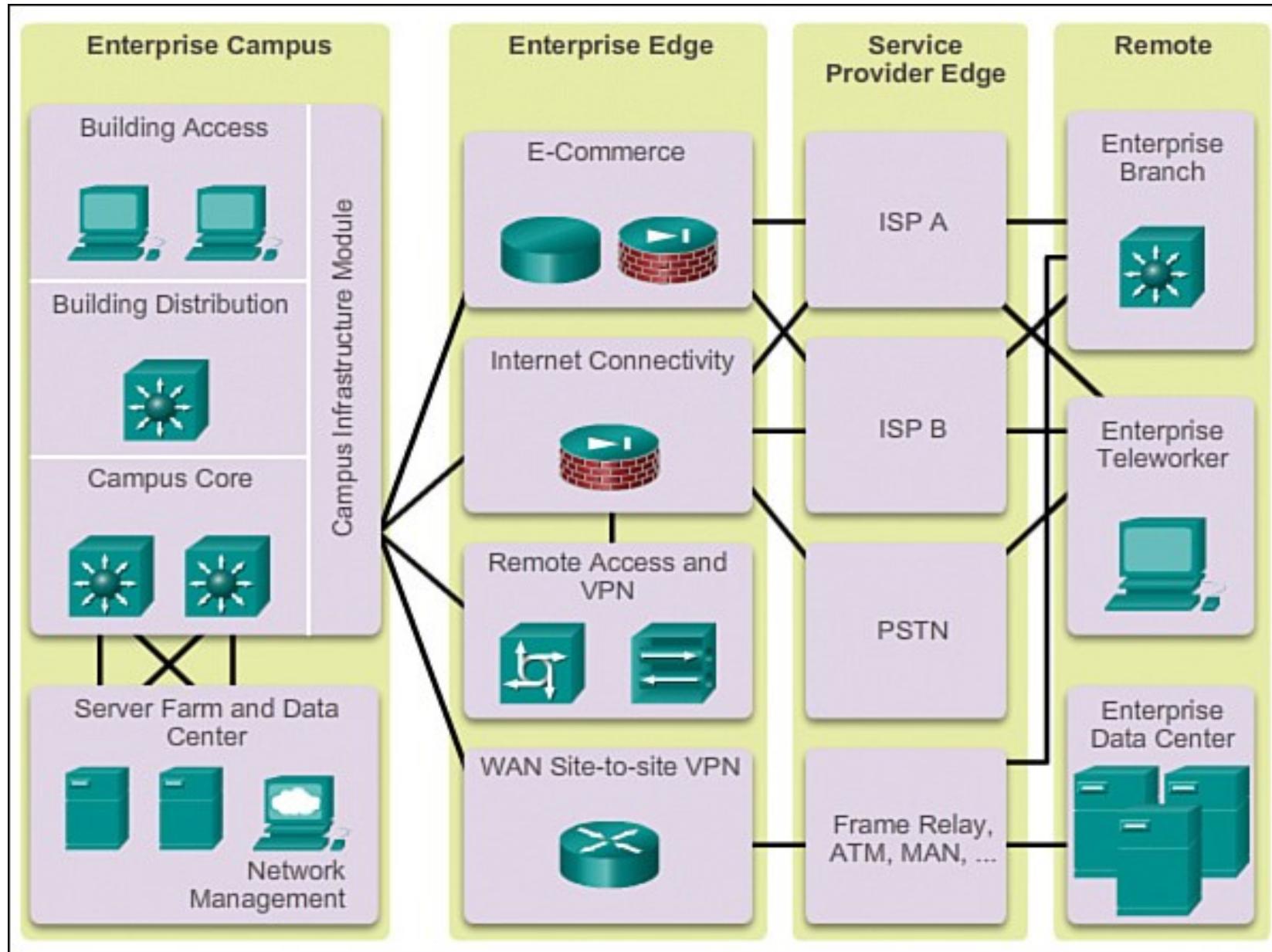
1. SOHO Network - Small Office /Home Office
2. Enterprise Network - MNC i.e. IBM, Intel, Infosys
3. Service Provider Network
 1. WAN SP, 2. ISP, 3. Cloud SP

Enterprise Network Infrastructure – 3 Blocks:

1. Campus Area Network
2. Data center
3. WAN - Service Provider



Enterprise Network Infrastructure



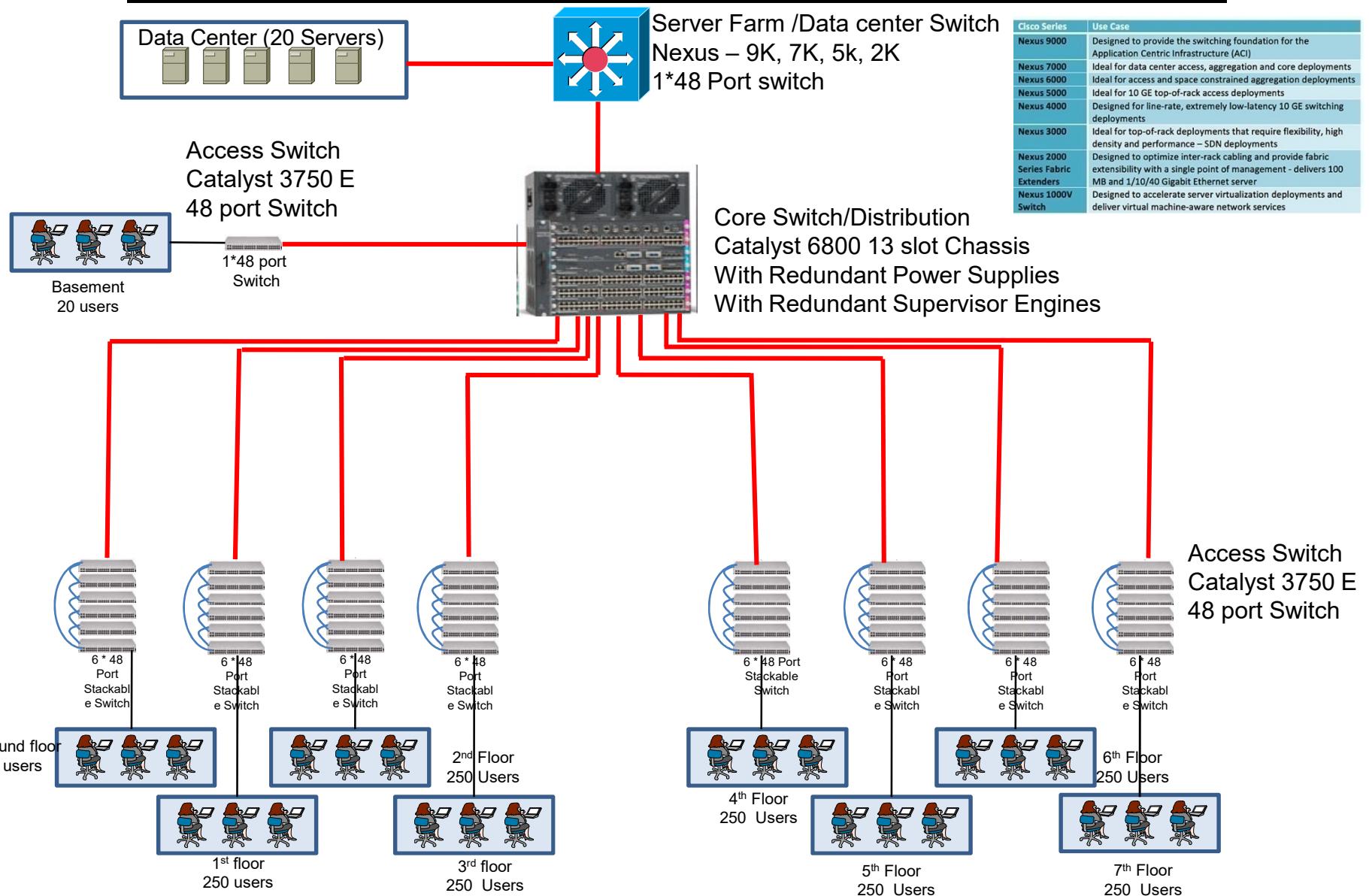
Network Fundamentals

Collapsed core and Three-tier architectures

Lesson 3

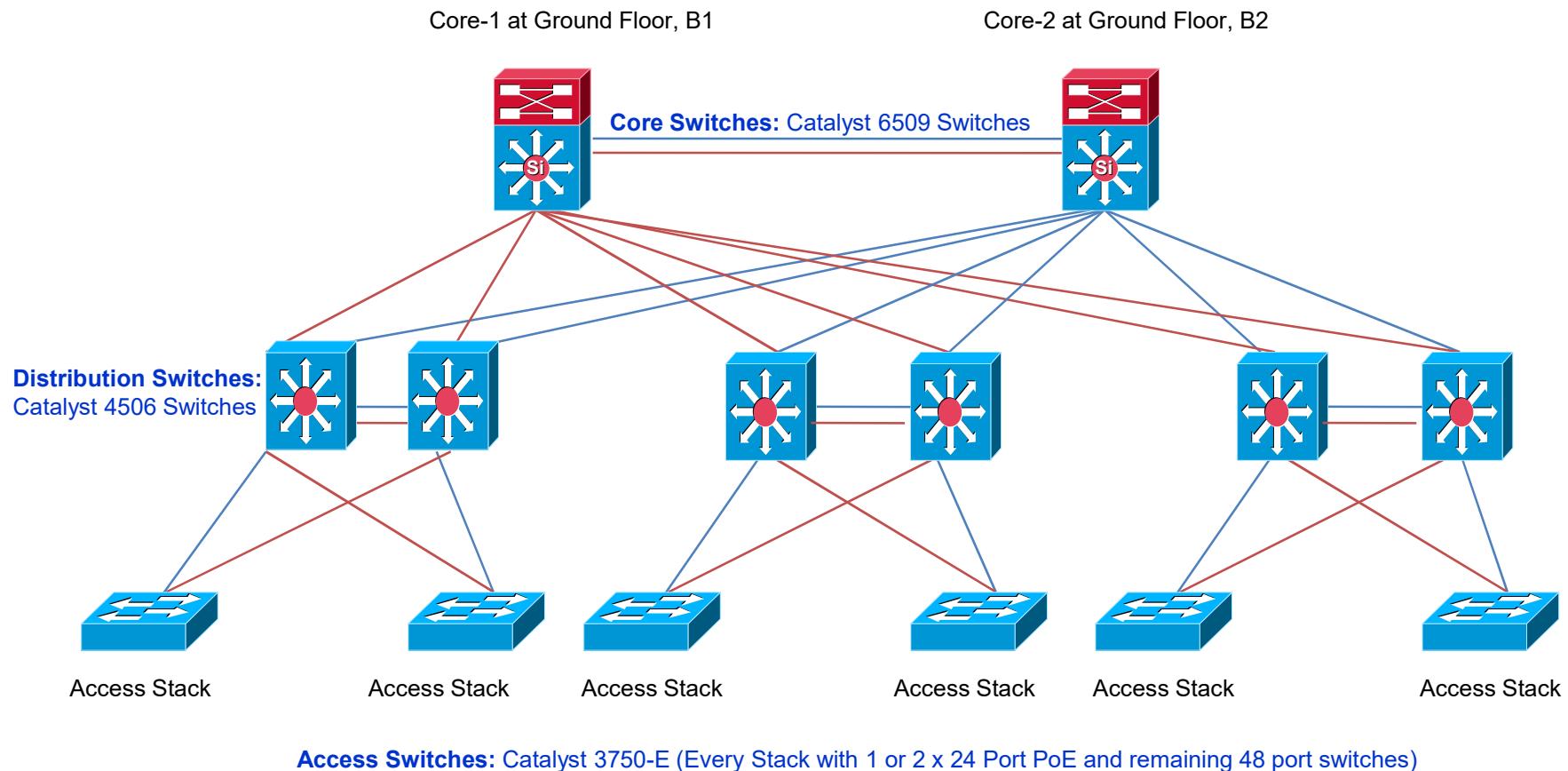


LAN - Collapsed Core Architecture



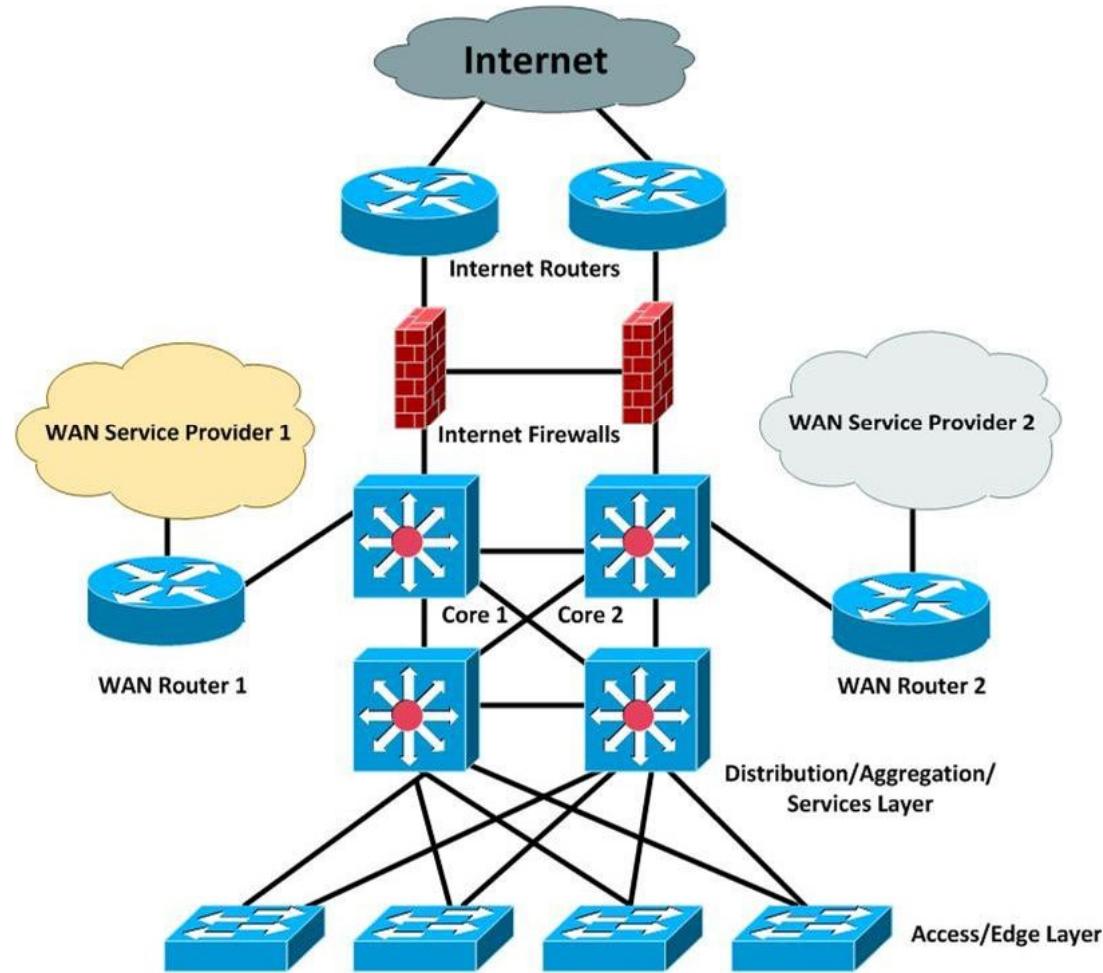
Cisco's Three Layer Hierarchical Model

- Cisco's Three tier/layer Hierarchical Model
 - Core Layer {Fast Switching}
 - Distribution Layer {Routing}
 - Access Layer {User connectivity}



Firewall

Enterprise Data Center



www.insearchoftech.com



kumar6009@gmail.com



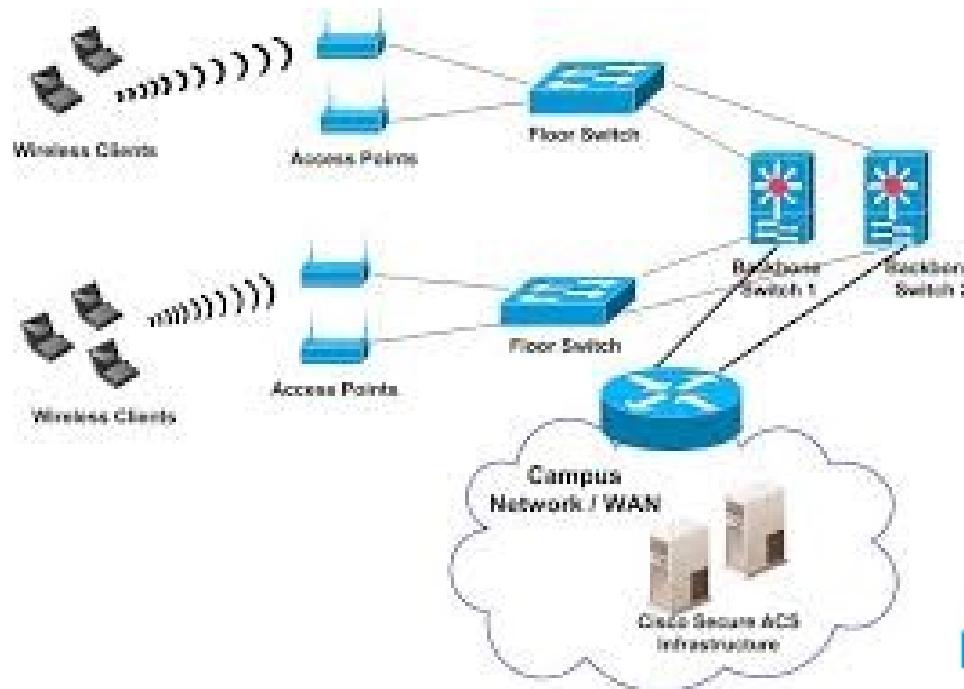
@air.ds2

Confidential and Need base circulation only

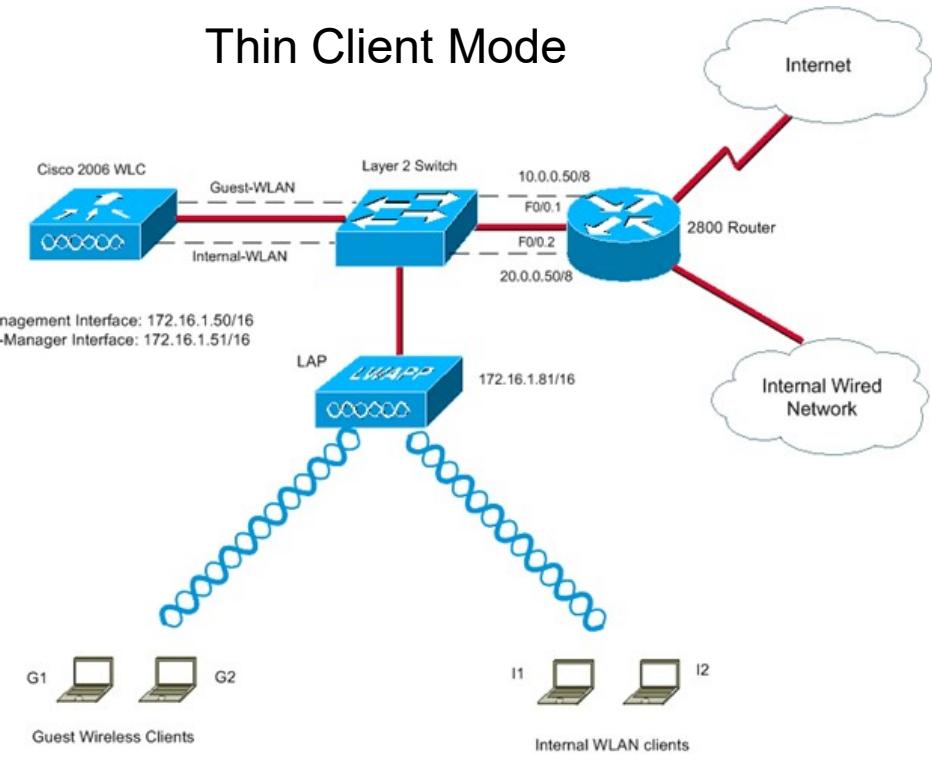
www.kumar6009.wixsite.com/ais3

Wireless Access point

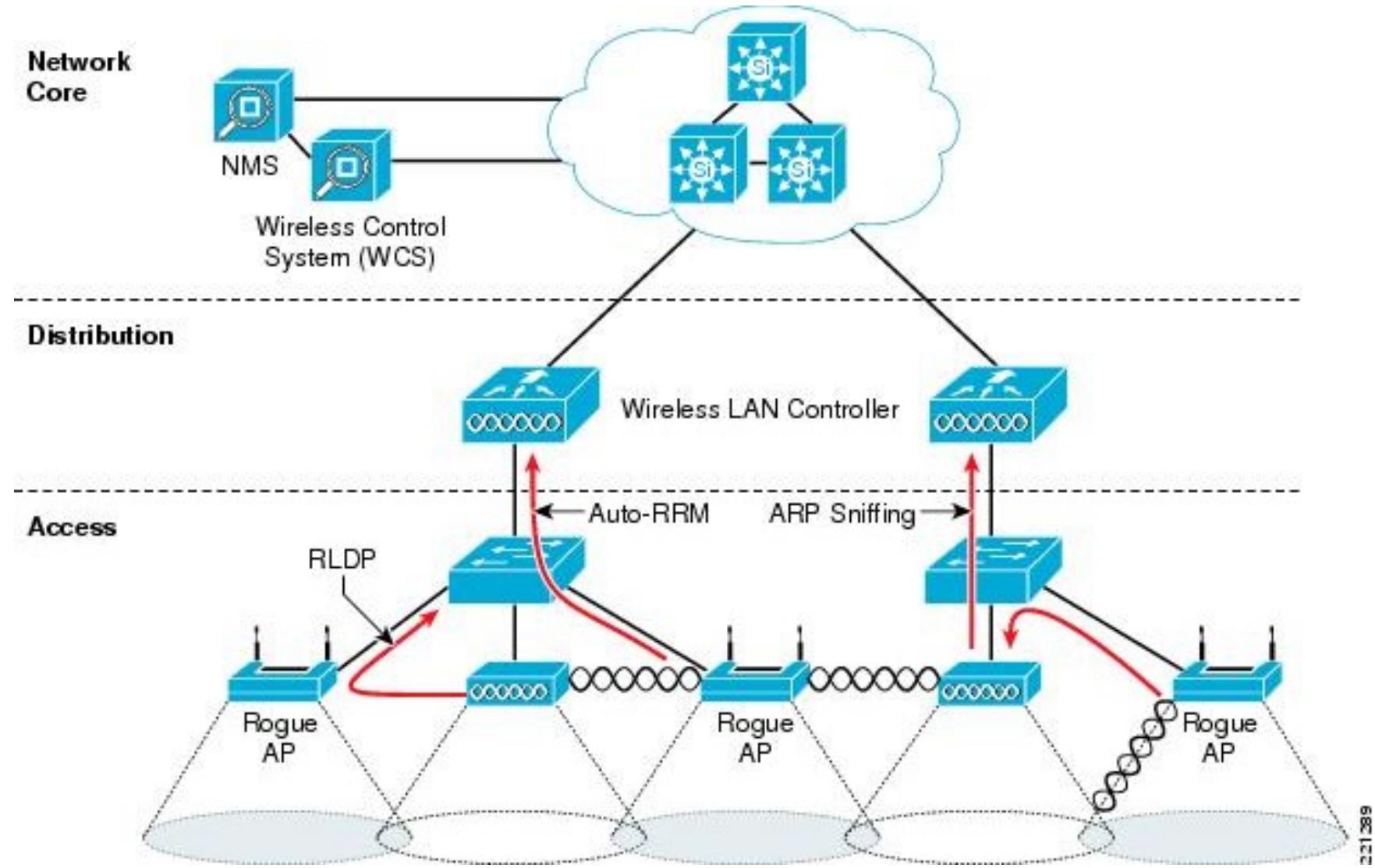
Autonomous Mode



Thin Client Mode



Wireless controller



221289



kumar6009@gmail.com



@air.ds2

Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3

Network Fundamentals

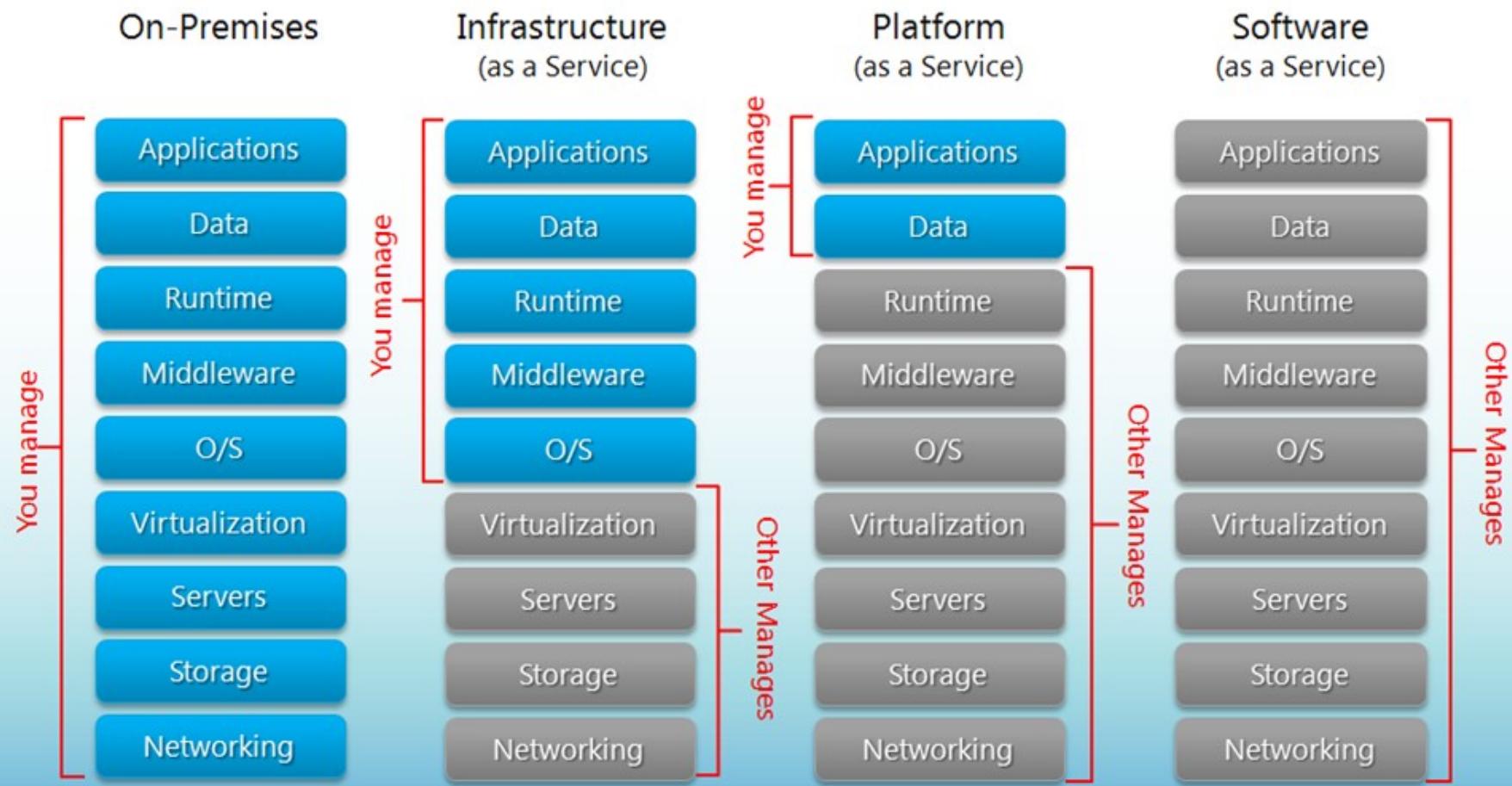
Cloud resources on enterprise network architecture

Lesson 3

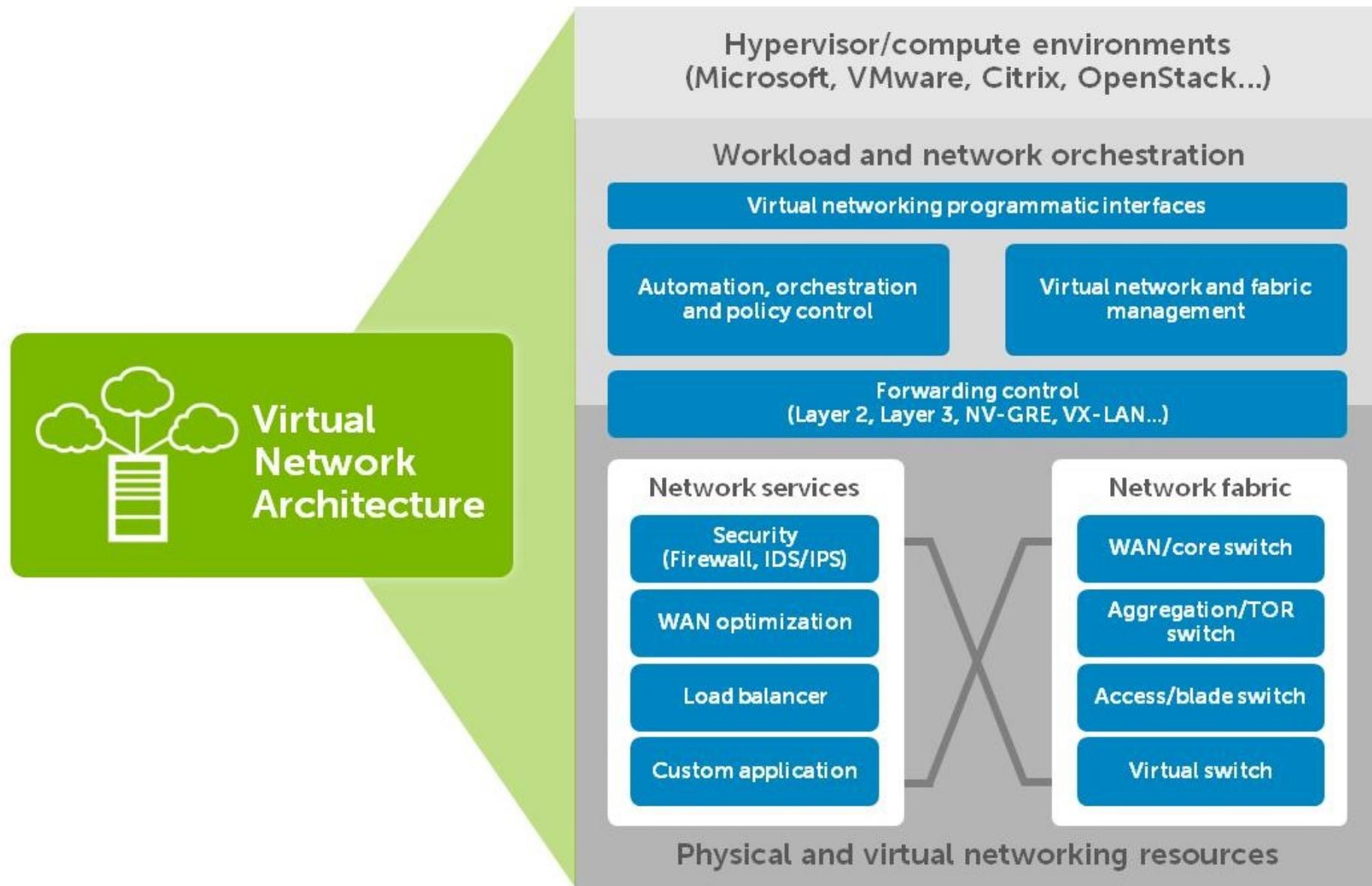


Cloud Models

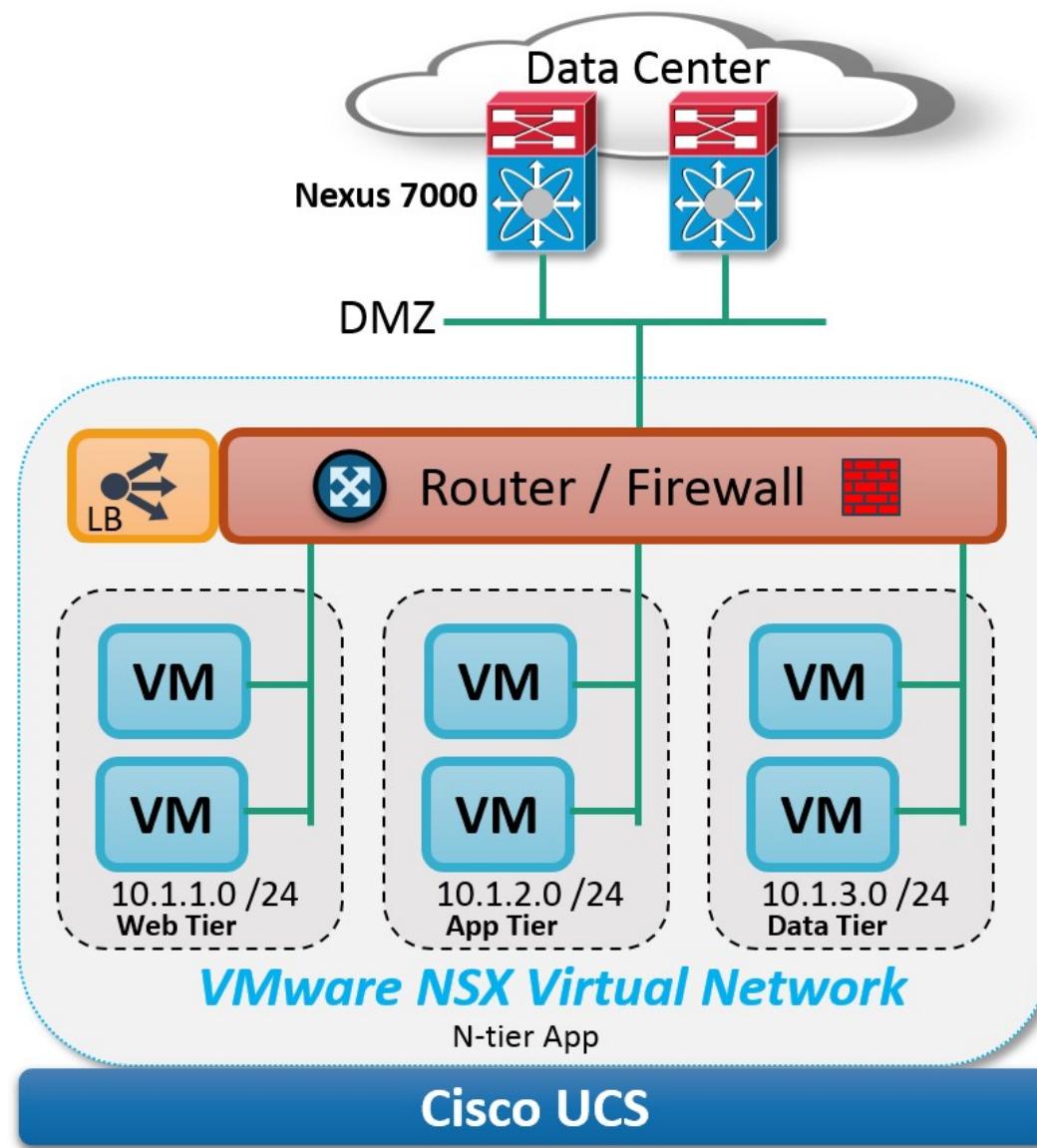
Separation of Responsibilities



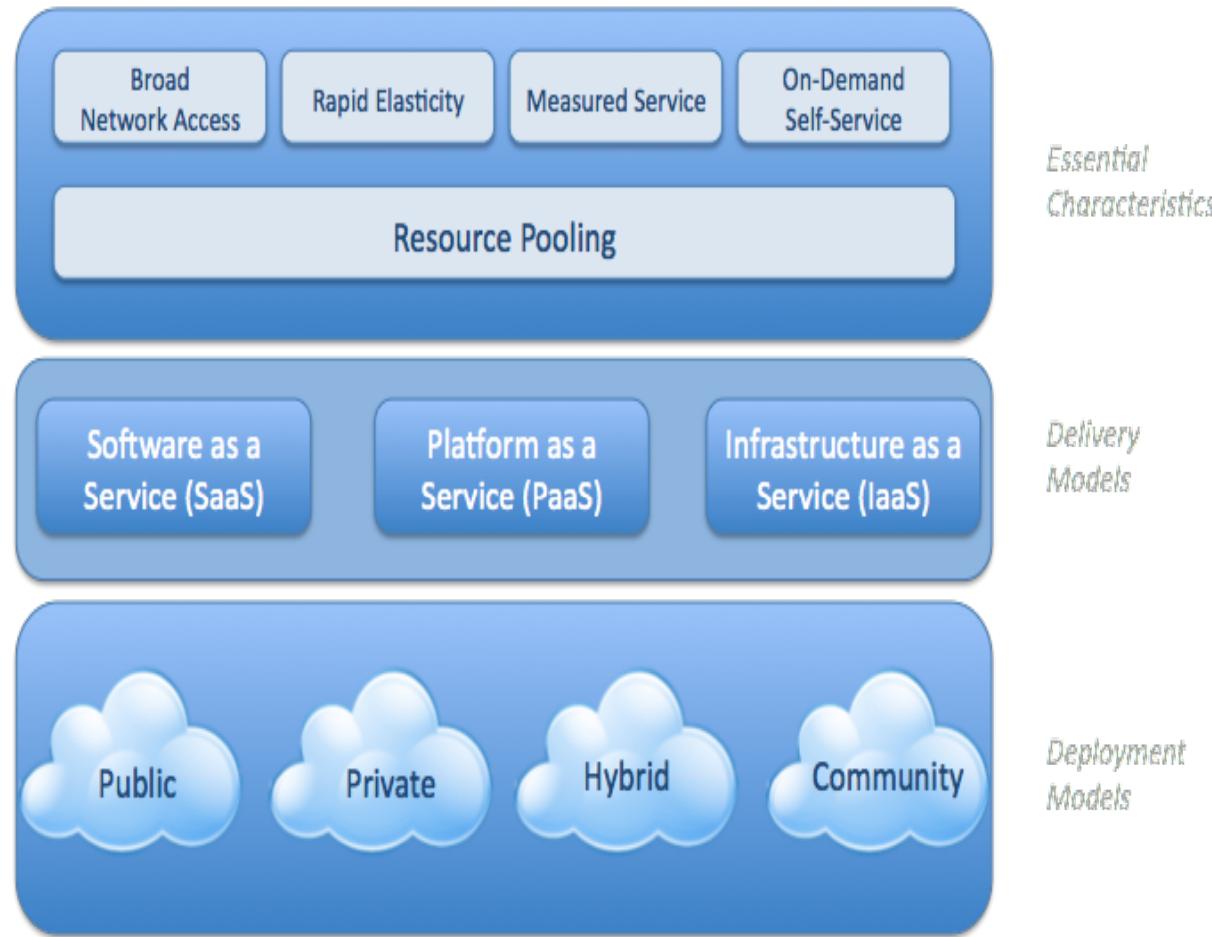
Enterprise network architecture



Enterprise network architecture



The technical View of Cloud



Visual Model of NIST Working Definition of Cloud Computing

<http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>



kumar6009@gmail.com

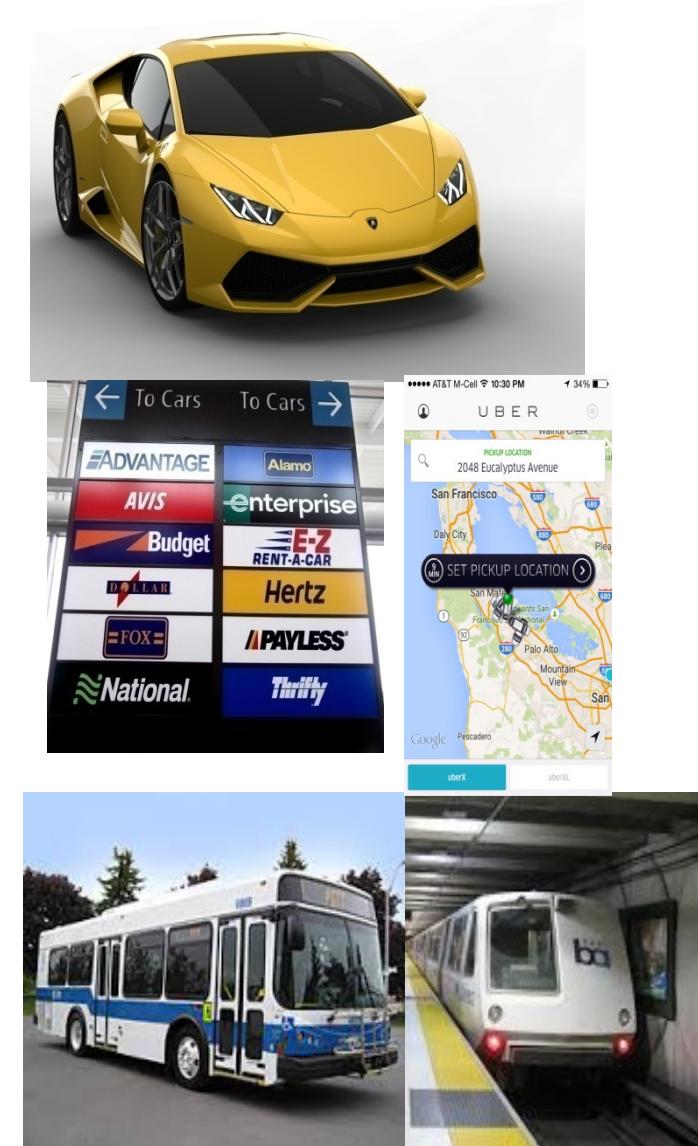
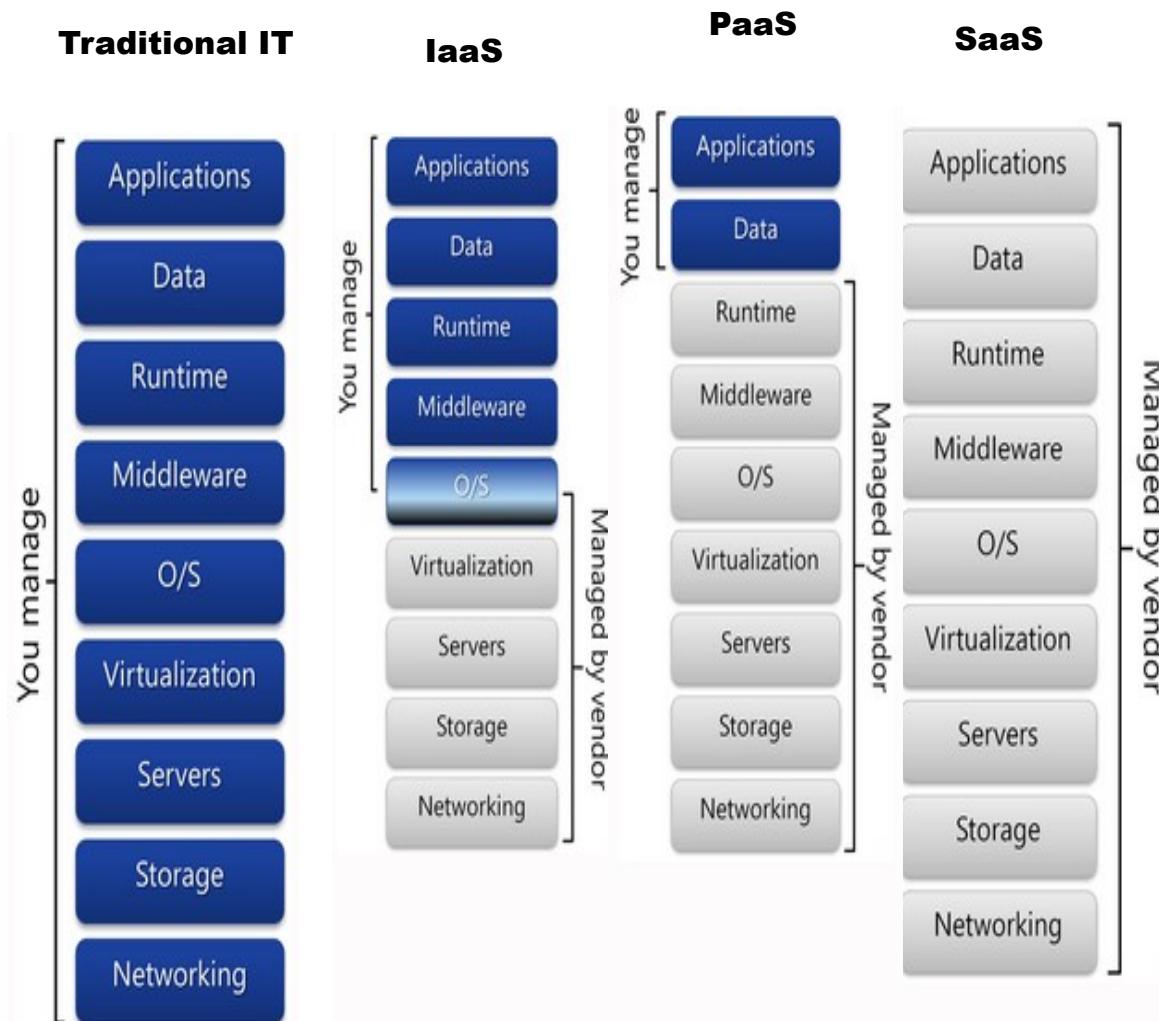


@air.ds2

Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3

SaaS, PaaS, IaaS Lots of *aaSes!



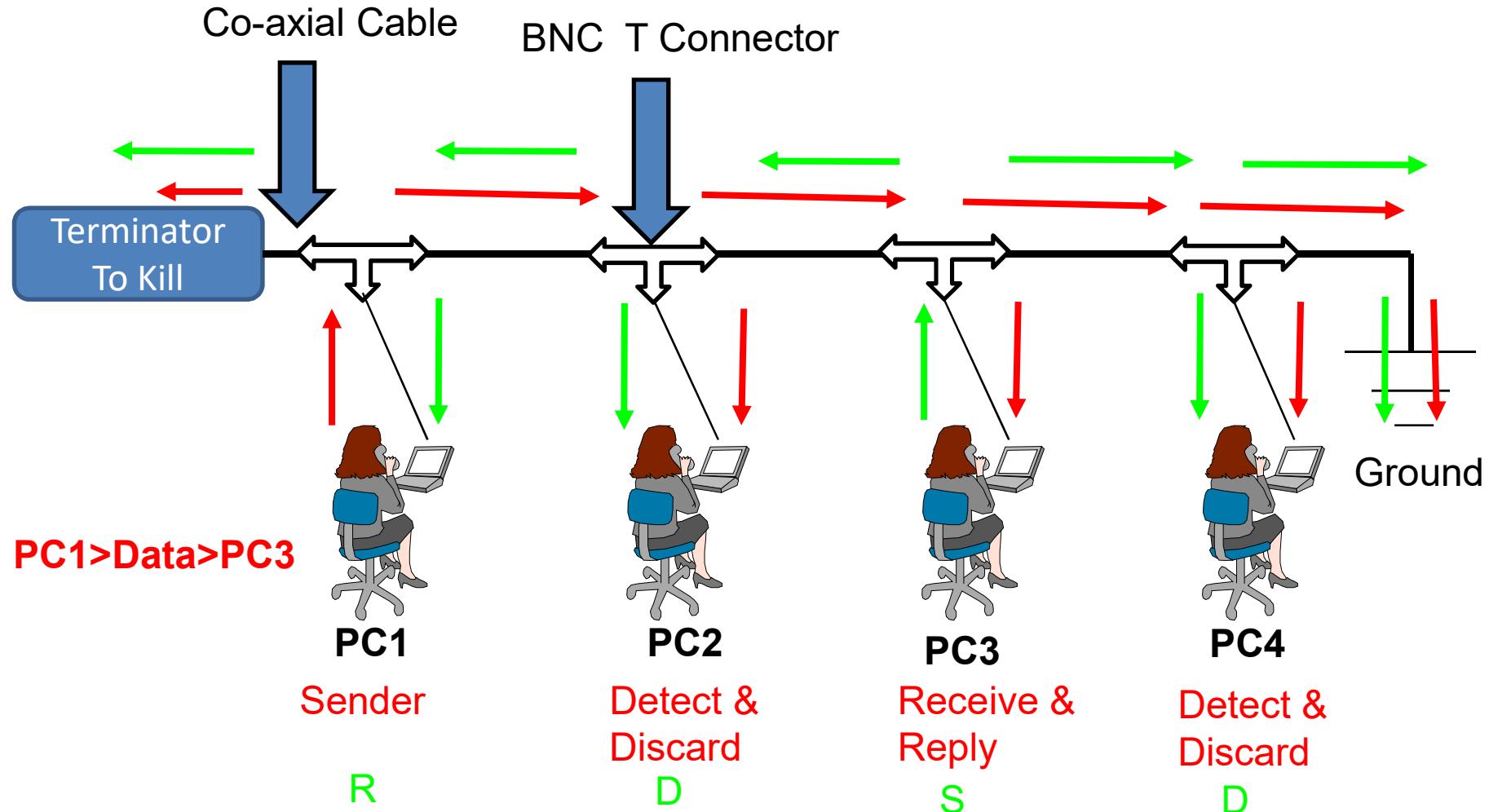
Network Fundamentals

Topologies

Lesson 7



Bus Topology



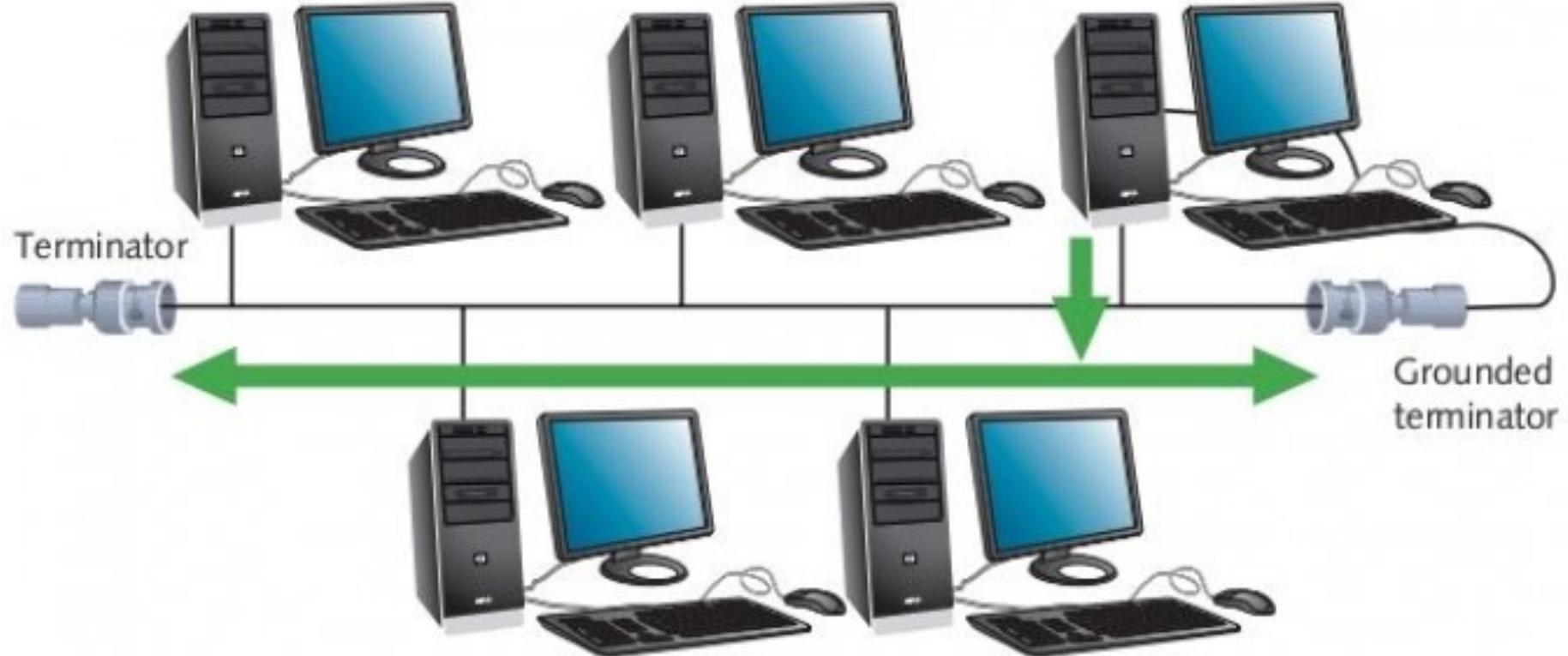
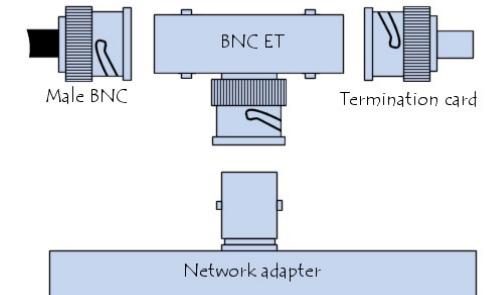
Bus Topology



BNC Barrel Connector

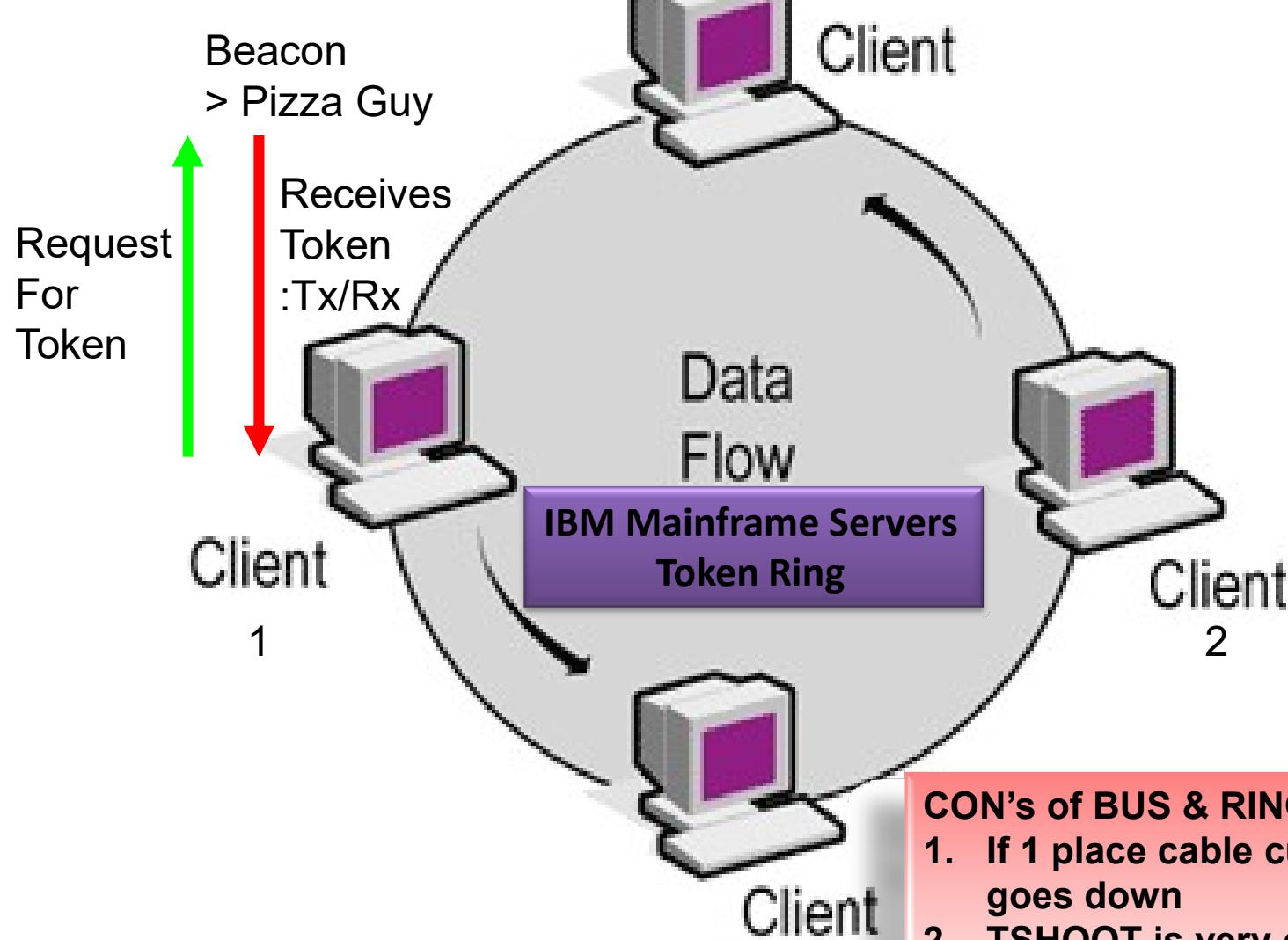


BNC T Connector



Ring Topology

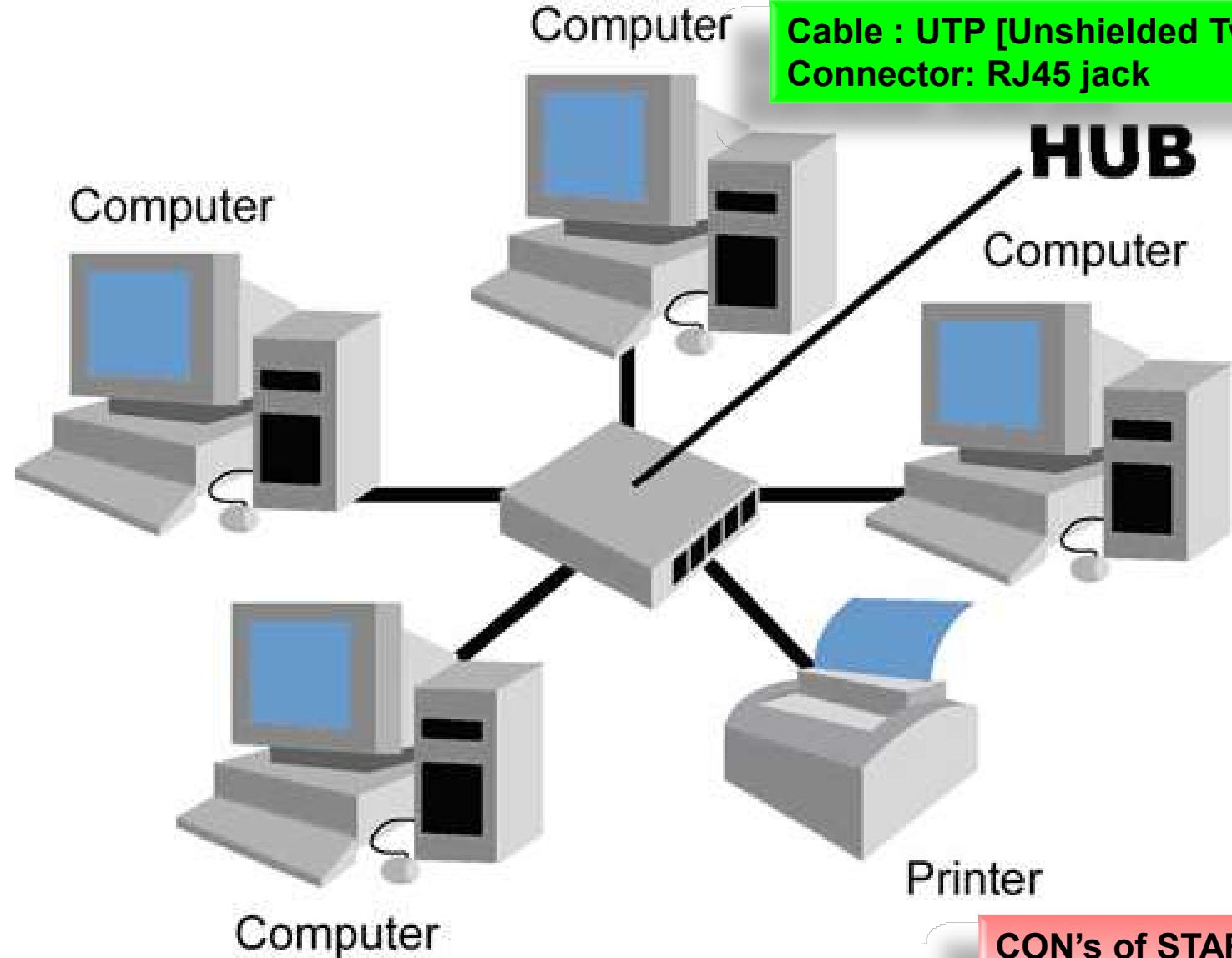
Special stream of Bits – Carrier signal



CON's of BUS & RING Topologies:

1. If 1 place cable cuts, whole NW goes down
2. TSHOOT is very difficult

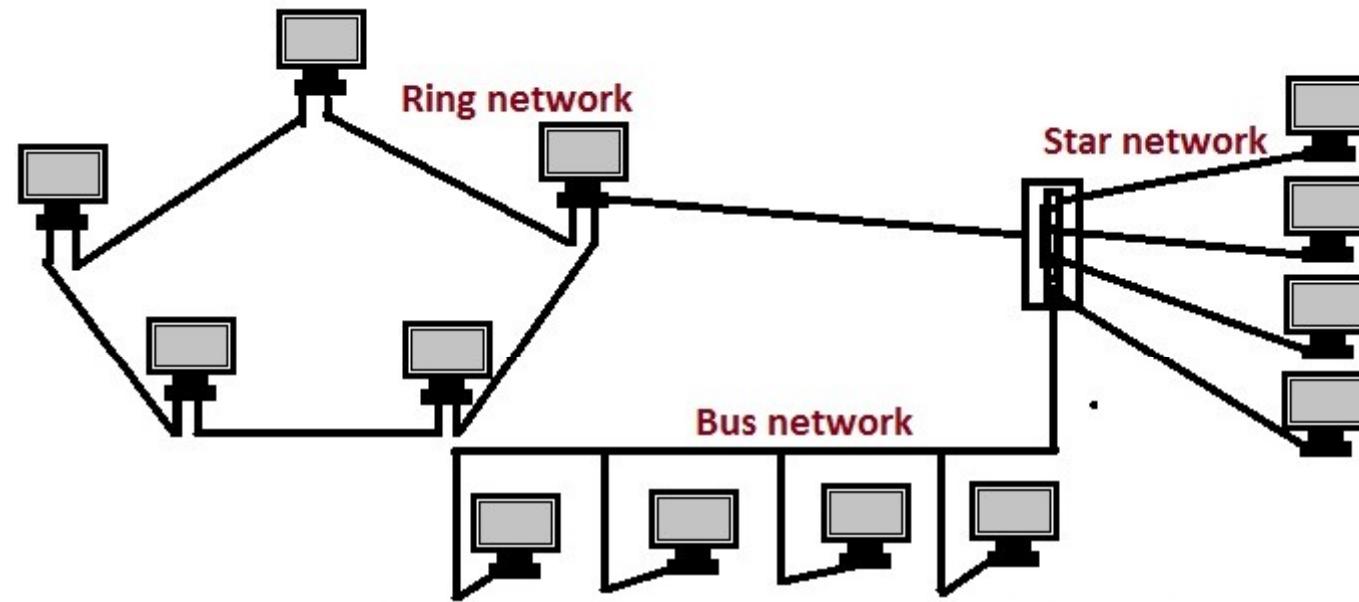
Star Topology



Printer

CON's of STAR Topology:
1. Single point of failure

Hybrid Topology



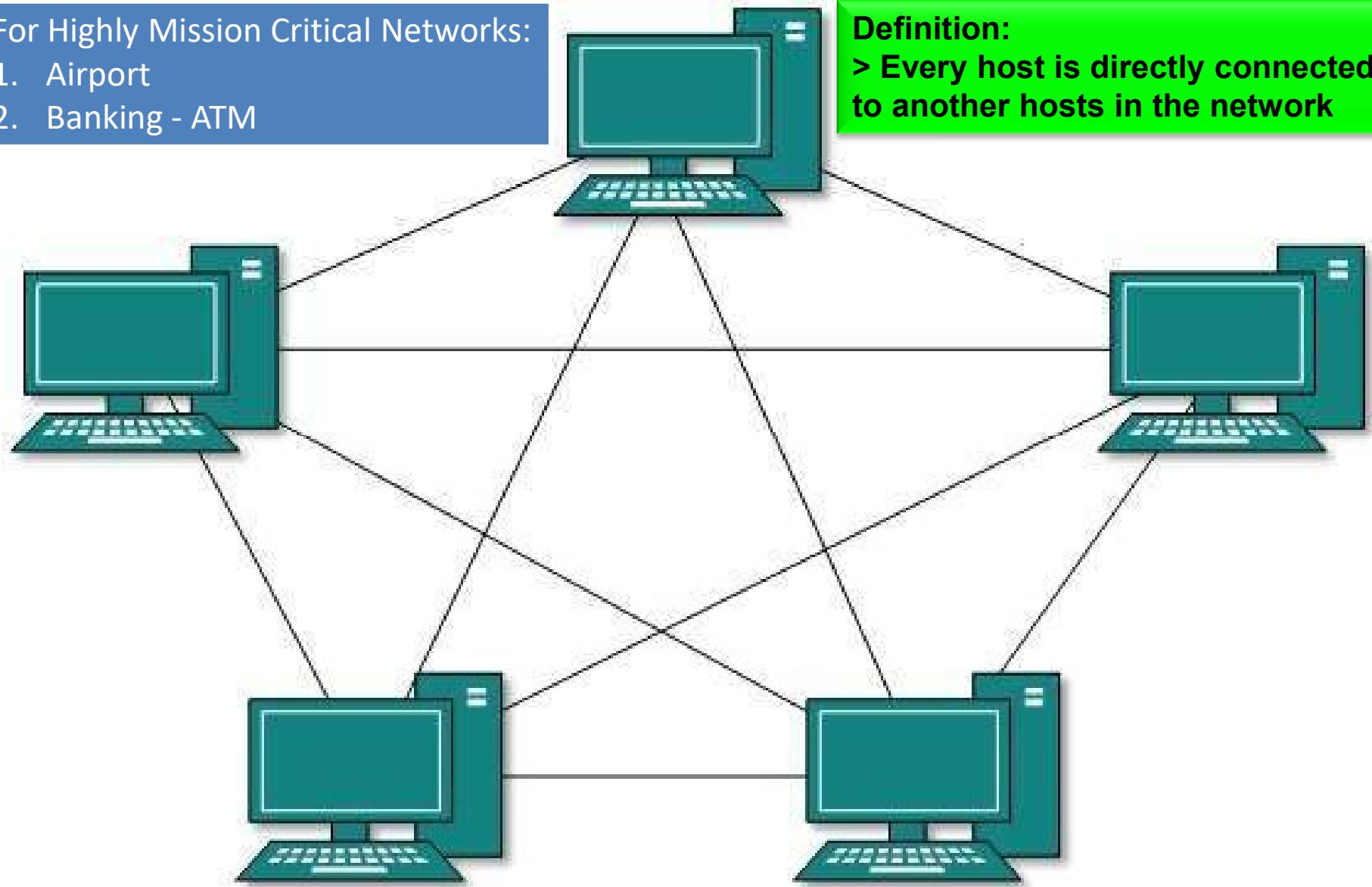
Mesh Topology

For Highly Mission Critical Networks:

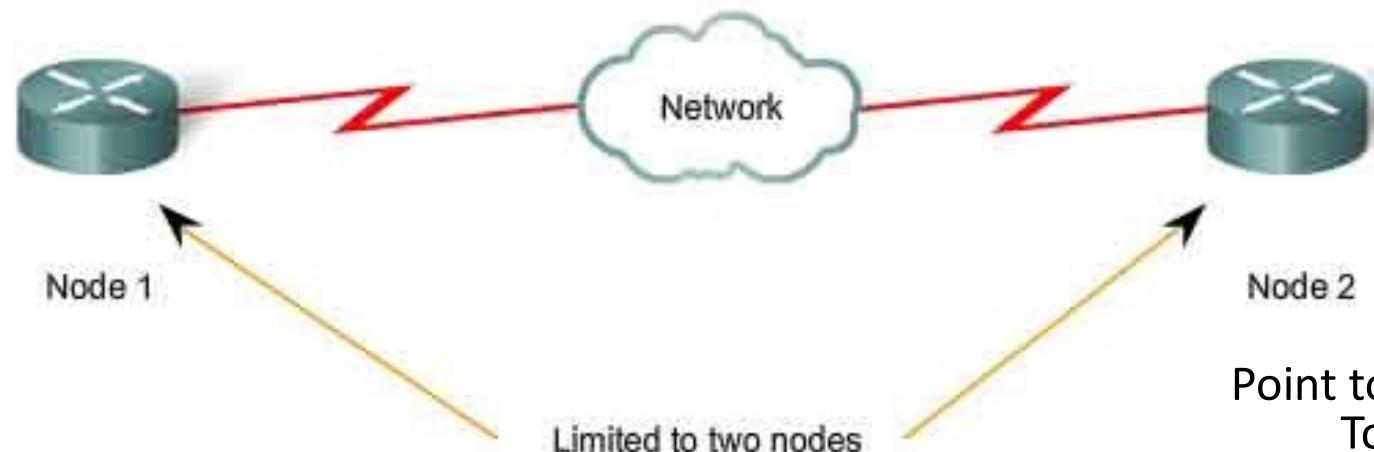
1. Airport
2. Banking - ATM

Definition:

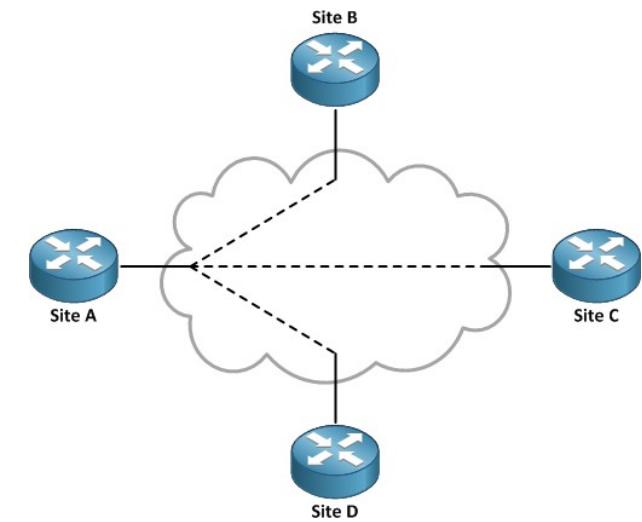
> Every host is directly connected to another hosts in the network



Point-to-Point Topology



Point to Multi-Point Topology



WAN Topology Types:

1. Hub & Spoke
2. Partial Mesh
3. Fully Mesh



kumar6009@gmail.com



@air.ds2

Confidential and Need base circulation only

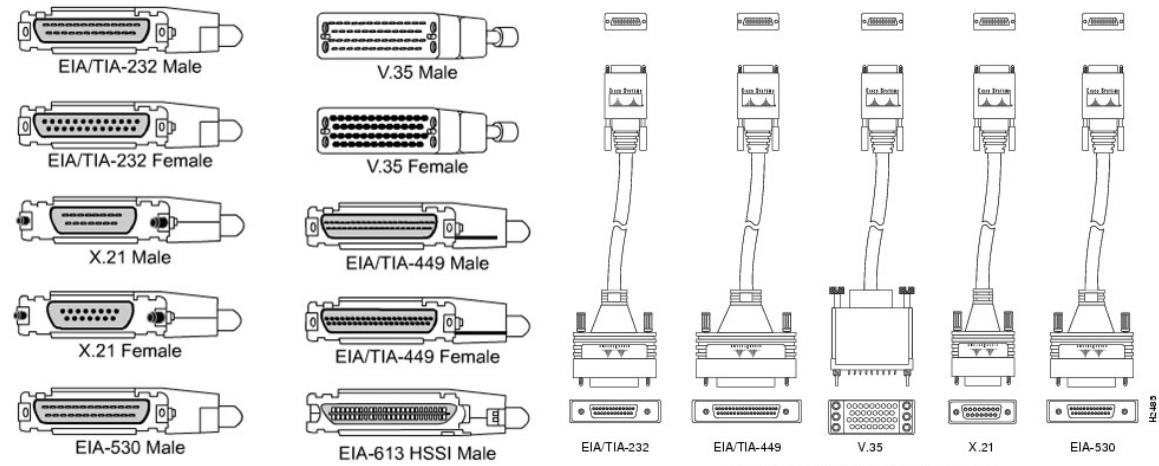
www.kumar6009.wixsite.com/ais3

76

Network Fundamentals

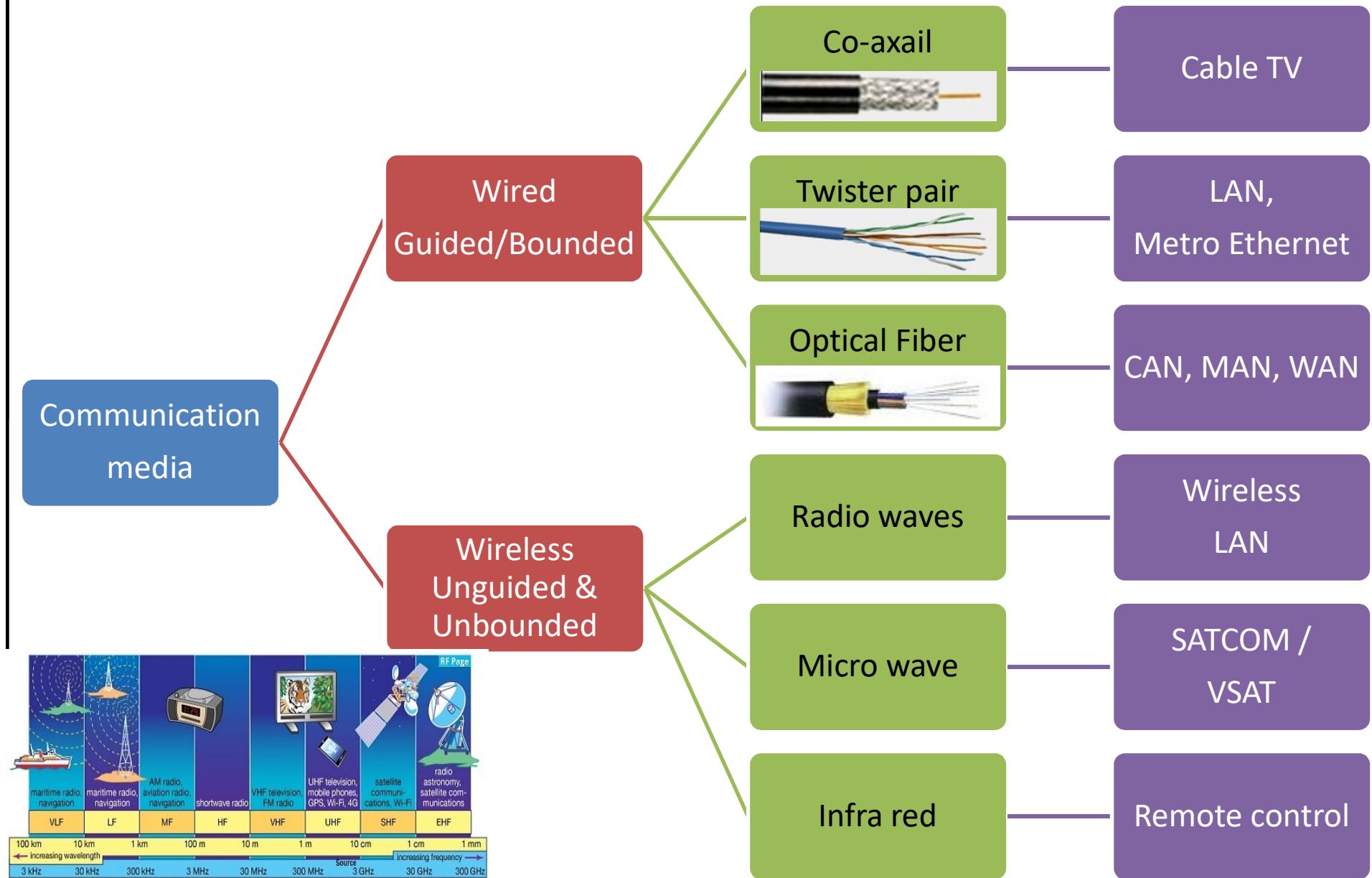
Media, Cable, port & connectors

Lesson 7



Network connections at the modem or CSU/DSU

Media, Cables, Ports & Connectors



Media, Cables, Ports & Connectors

Cables

- **Wired Communication Media**

- **Coaxial Cable**

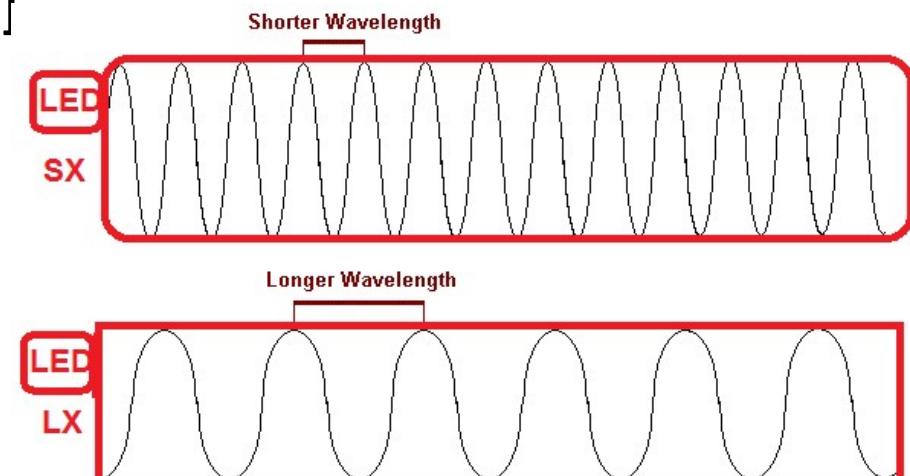
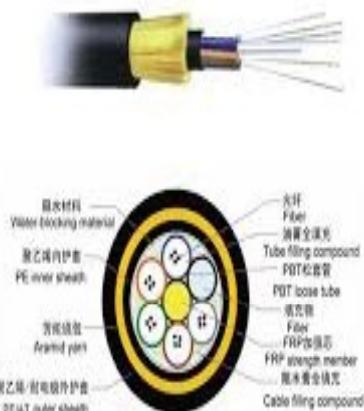
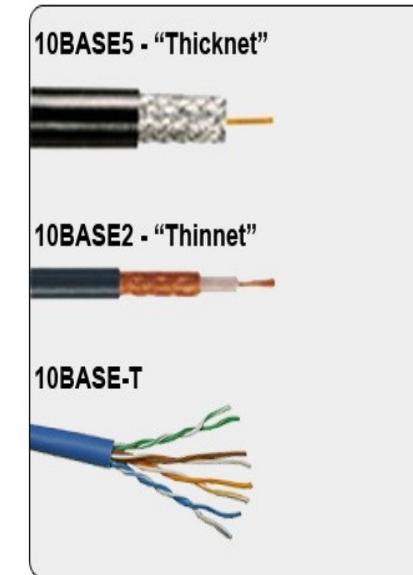
- **10Base 2 – Thin Net**
- **10Base 5 – Thick Net**

- **Twisted pair cable**

- **10Base T [Ethernet]**
- **100 Base T [Fast Ethernet]**
- **1000 Base T [Gigabit Ethernet]**

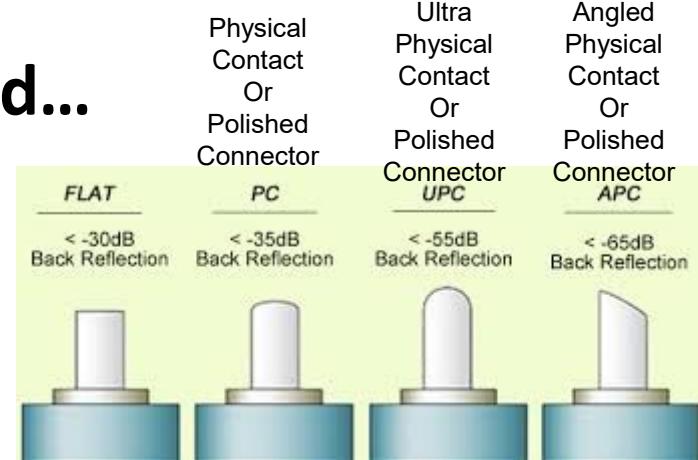
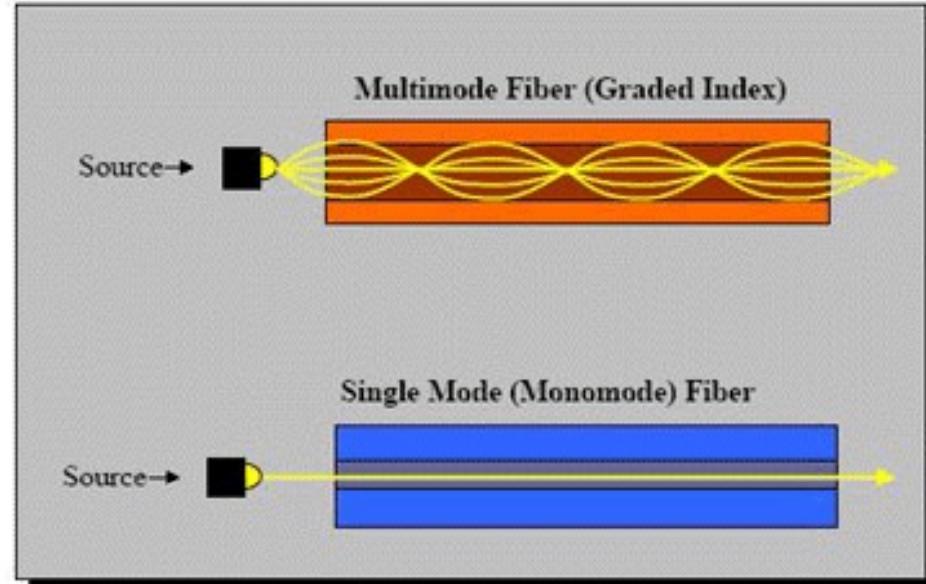
- **Fiber Optic Cable**

- **1000 Base SX**
- **1000 Base LX**
- **Single Mode Cable**
- **Multi Mode Cable**



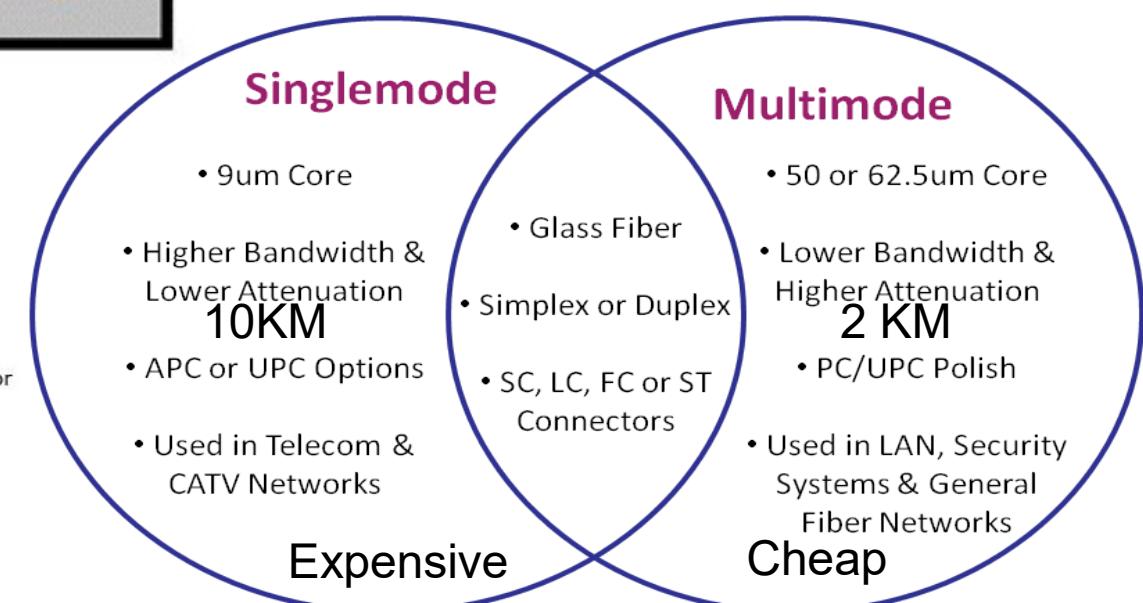
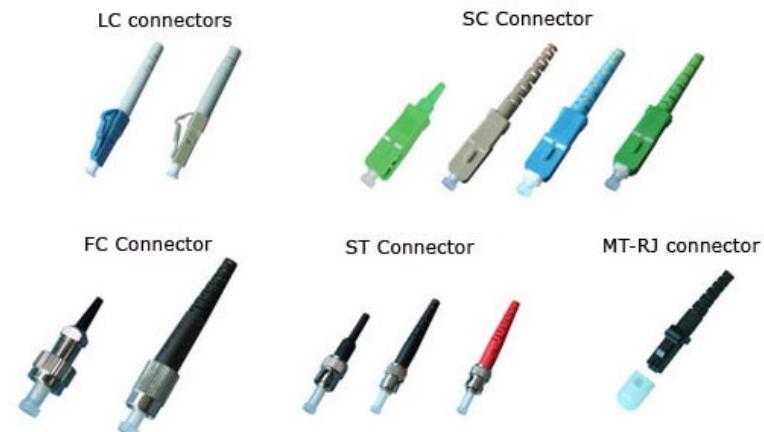
Media, Cables, Ports & Connectors

Cables contd...



Which is best for Implementation:

- As a solution Multimode is cheaper;
- As a complete solution Single mode is expensive



Media, Cables, Ports & Connectors

Cables contd...

Unshielded Twisted Pair [UTP]

1. Roll over cable/ Flat Cable / Console cable
 - PC to Switch Console Port
 - PC to Router Console Port

2. Straight Through Cable
 - Dissimilar/Different Devices
 - Switch to PC
 - Router to Switch

3. Cross over Cable
 - Similar/Same Devices
 - Switch to Switch
 - PC to PC

- PC{router} to Router → CO Cable
- Exception – PC has routing Functionality

Twisted Pair:

1. Shielded Twisted Pair (STP)
 - Industrial nw & R&D labs
2. Unshielded Twisted Pair (UTP)
 - General Networks i.e. LAN



Media, Cables, Ports & Connectors

Cables contd...

TIA/EIA 568A Wiring

1	White and Green
2	Green
3	White and Orange
4	Blue
5	White and Blue
6	Orange
7	White and Brown
8	Brown

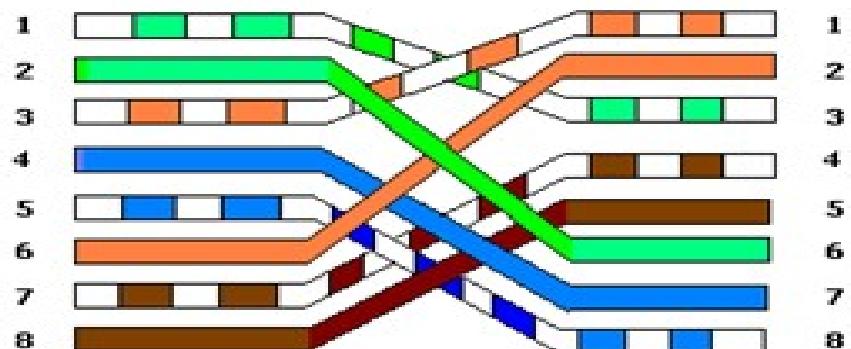
TIA/EIA 568B Wiring

1	White and Orange
2	Orange
3	White and Green
4	Blue
5	White and Blue
6	Green
7	White and Brown
8	Brown

Figure A

Shows the Pin Out of Straightthrough Cables

TIA/EIA 568A Crossed Wiring



TIA/EIA 568B Crossed Wiring

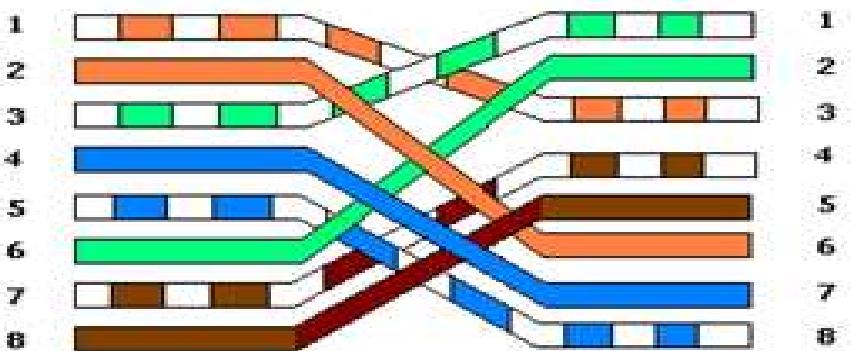


Figure B

Shows the Pin Out of Crossover Cables

Telecommunications Industry Association (TIA) Electronic Industries Alliance (EIA)



kumar6009@gmail.com



@air.ds2

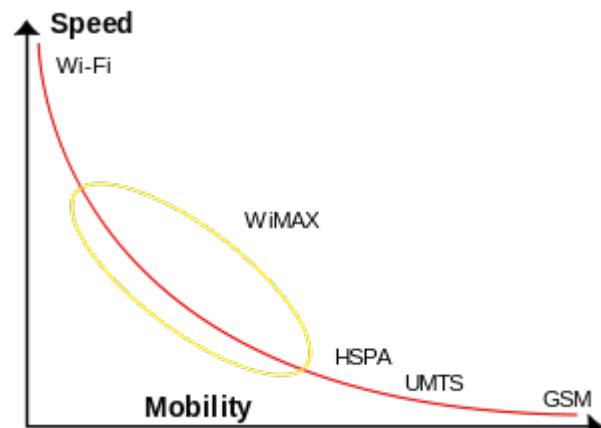
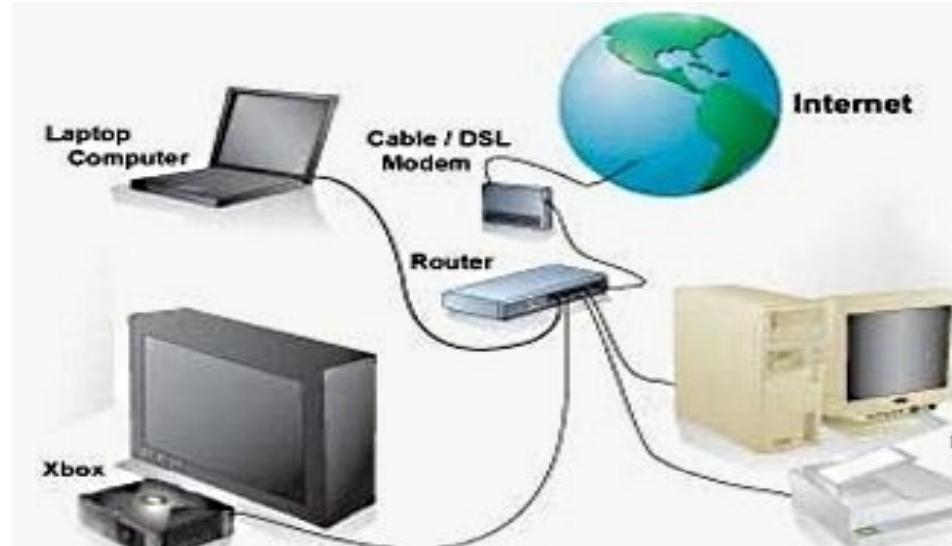
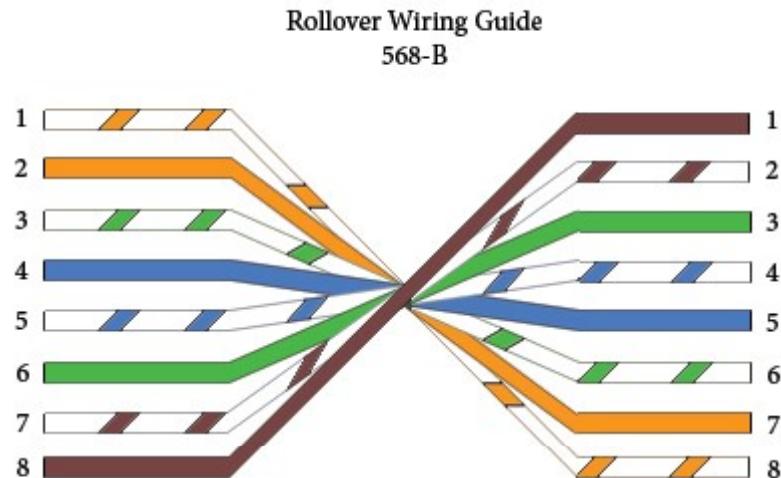
Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3

82

Media, Cables, Ports & Connectors

Cables contd...



Wired vs. Wireless [Consumer / Personal use applications]		
	Wired	Wireless
Convenience	★★	★★★★★
Reliability	★★★★★	★★★★★
Speed	★★★★★	★★★★★
Security	★★★★	★★★
Ease of initial Setup	★★★★★	★★★★

<http://customcable.ca>



Media, Cables, Connectors & Ports

Ports {Interfaces}

- **LAN Interfaces**
 - Ethernet Ports {10Mbps} i.e. e0, e1 or e0/0, e0/1
 - Fast Ethernet Ports{100 Mbps} i.e. fa0, f1 or f0/0, f0/1
 - Gigabit Ethernet Ports{1000 Mbps} i.e. Gig 0/0, G0/1
- **WAN Interfaces**
 - Serial Ports i.e. S0, S1 or S0/0 , S0/0/0
 - ISDN BRI Ports i.e. Bri.2/0,
 - ISDN PRI Ports i.e. Pri.2/0
 - E1/T1 ports

Media, Cables, Ports & Connectors

Connectors

RJ - 45



RJ - 11

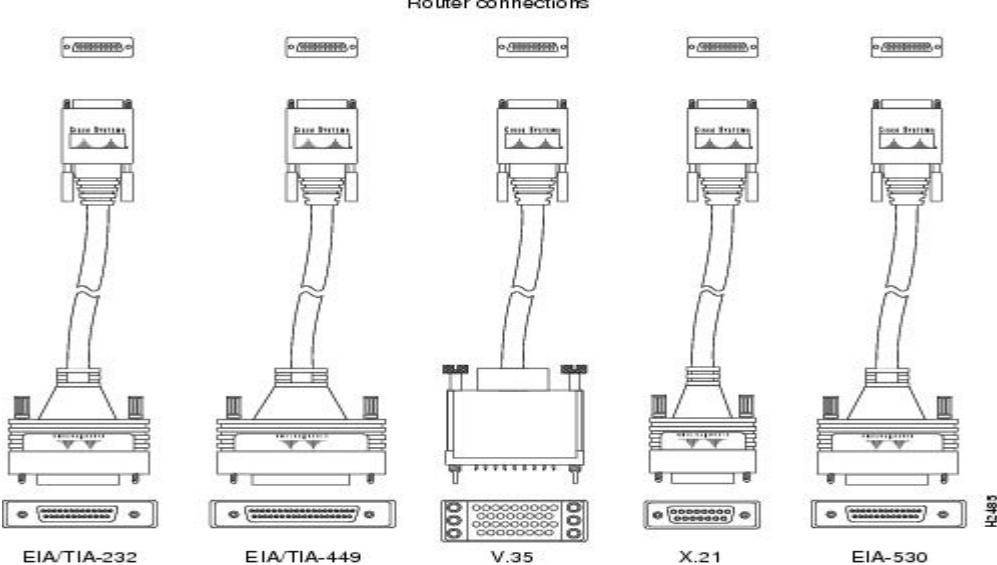


DB9 Connectors



female

male



Network Fundamentals

Troubleshooting Approach & methodologies to resolve problems

Lesson 8



Introduction

- Defining Troubleshooting
 - Skills
 - Data>Information>knowledge>practice>Problem solving skills>Wisdom > Wise
 - No right way or wrong way
 - Efficient & effective way
 1. Defining the issue
 1. I/p & o/p criteria
 2. Gathering information
 3. Propose an hypothesis
 4. Temporary fix(Work Around)- until – permanent fix



Problem: STP
Solution:
Temp Fix - Remove redundant cable
Perm Fix – Reconfigure STP

Problem Report

Problem Diagnosis

Problem Resolution

Steps to Diagnose a problem

Steps	Description
1) Collect Information	Tools/Interview users
2) Examine Collected Information	Compare info with baseline
3) Eliminate Potential Causes	Knowledge & interrogation
4) Propose an hypothesis	Most likely cause of the problem
5) Verify hypothesis	Test its theory (POC)

Ticket 2:
Toaster Problem



Troubleshooting in 7 Steps

Step 1 : Problem report (i/p & o/p criteria) [Pr]

Step 2 : Collect Information [CI]

Step 3 : Examine Collected Information [EI]

Step 4 : Eliminate potential Causes [EP]

Step 5 : Propose an hypothesis [PH]

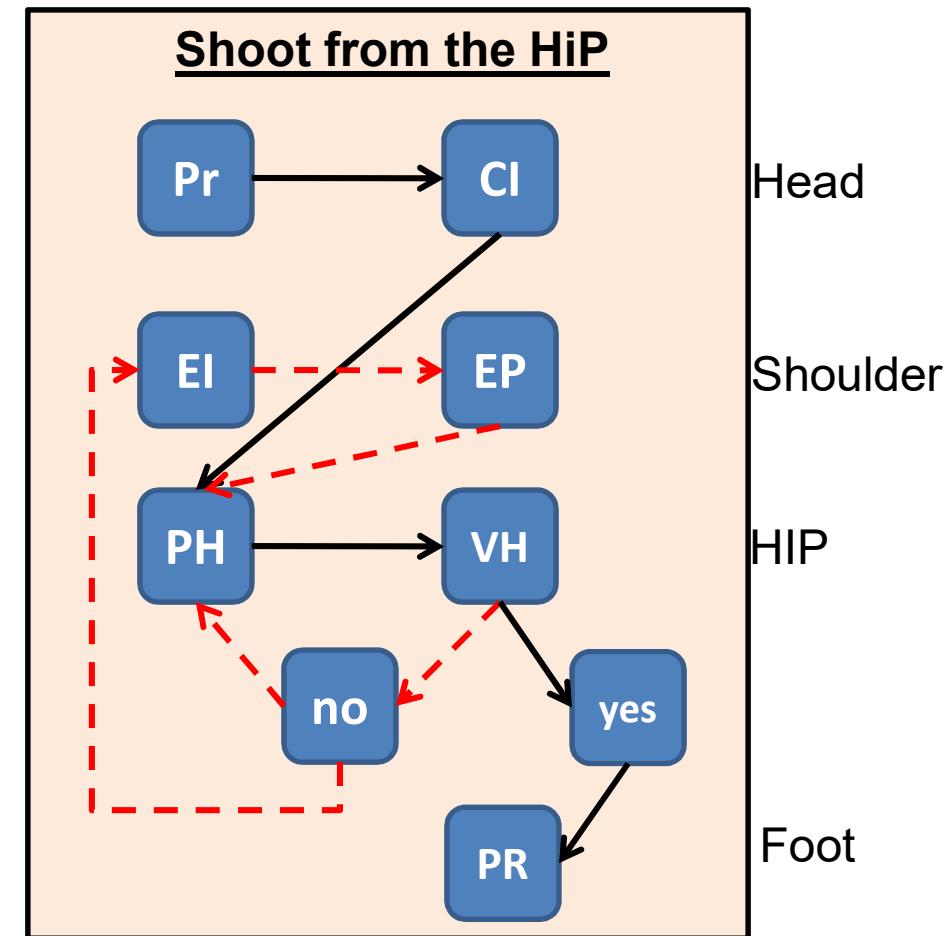
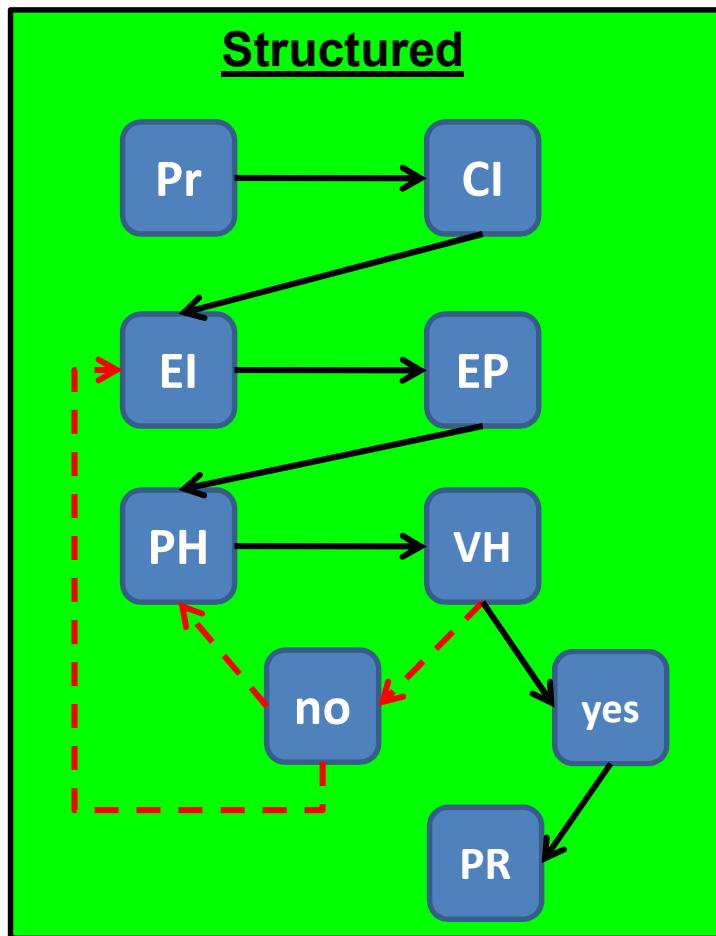
Step 6 : Verify hypothesis i.e. POC, Pilot [VH]

Step 7 : Problem Resolution [PR]

Work-Around{OPM} & Permanent Solution

The Value of Structured Troubleshooting

1. Structured Troubleshooting Approach
2. HiP Troubleshooting Approach



Popular Troubleshooting Methods

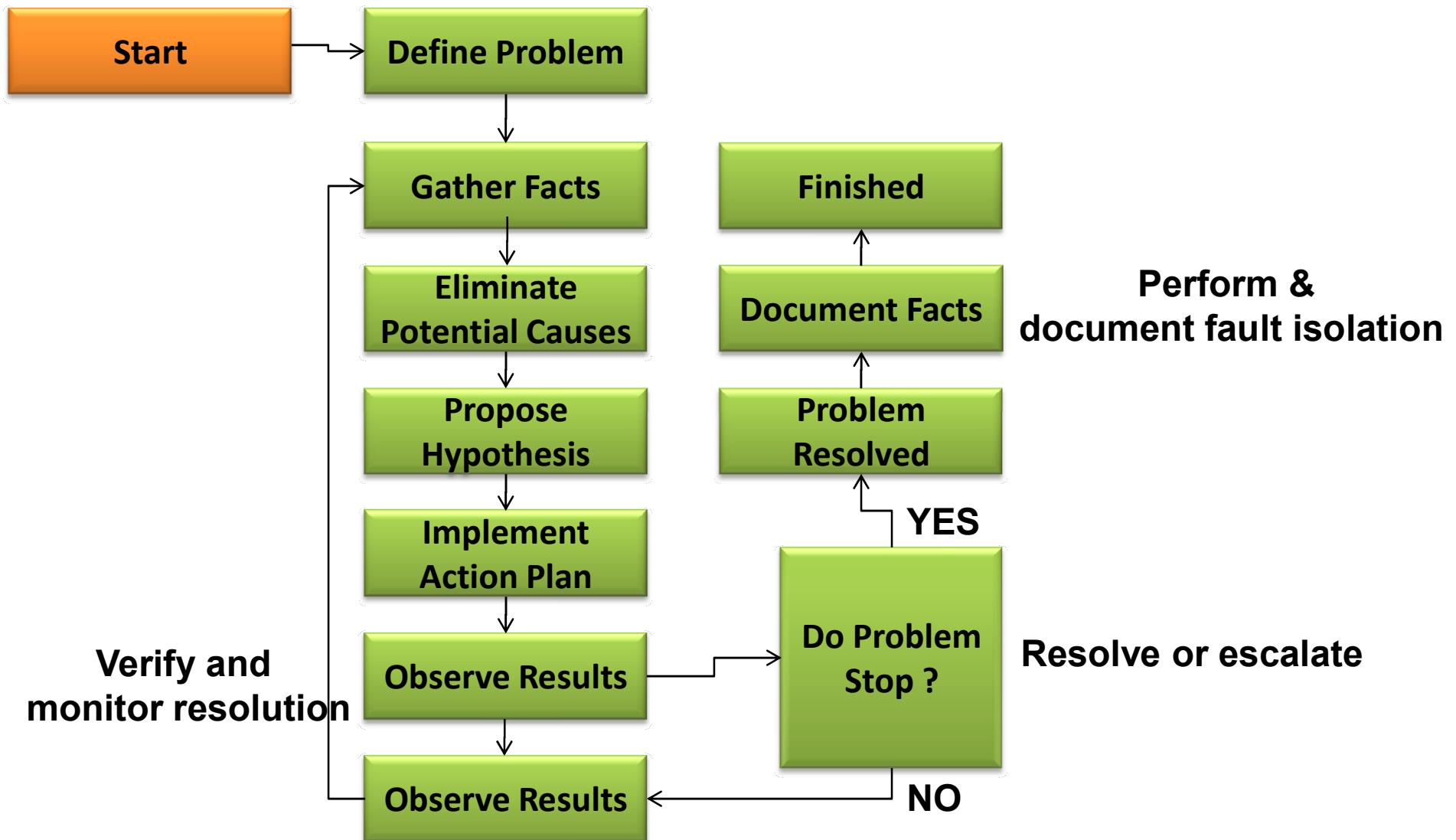
1. The top-down method (L7 to L1)
2. The bottom-up method (L1 to L7)
3. The divide – and – conquer method
 - Ping reply – yes – Problem in Upper layer (L5 to L7)
 - Ping unreachable - Problem in Lower layer (L1 to L4)
4. Following the traffic path
 - Ping from source to destination hop by hop in the path of data flow
5. Comparing configurations
6. Component swapping

For Life Problems: Permanent fix: Self-Enquiry of Who am “I”?

**The one, who sees In Every Opportunity only difficulties is called Pessimist.
The one, who sees In Every Difficulty only Opportunities is called Optimist.**

Just Be Honest to Your-Self ☺ That's all .

Troubleshooting methodologies



Network Fundamentals

IP Addressing {IPv4}

Lesson 8

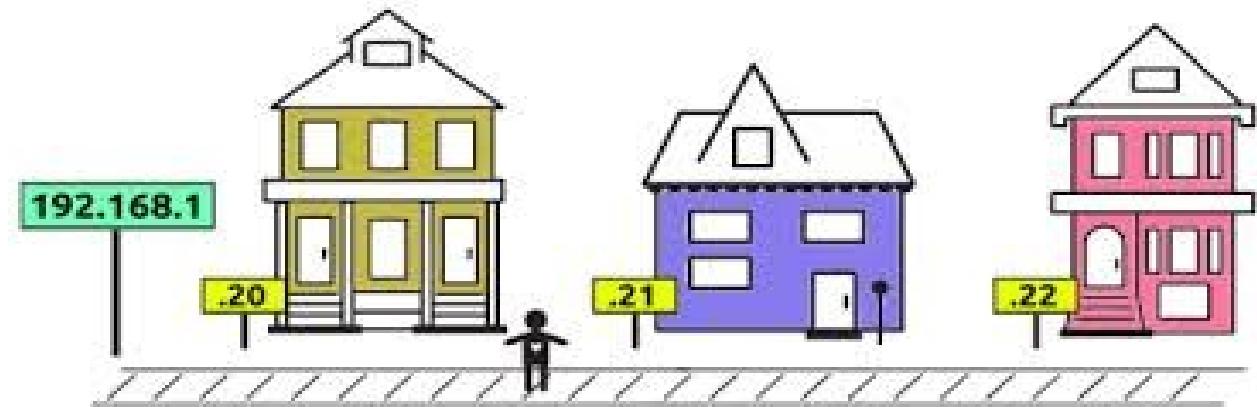


Table of Contents

3.0 IP Addressing (IPv4/IPv6)

3.1 Describe the operation and necessity of using private and public IP addresses for IPv4 addressing

3.2 Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment

3.3 Identify the appropriate IPv4 addressing scheme using VLSM and summarization to satisfy addressing requirements in a LAN/WAN environment

3.4 Describe the technological requirements for running IPv6 in conjunction with IPv4

 3.4.a dual stack

3.5 Describe IPv6 addresses

 3.5.a global unicast

 3.5.b multicast

 3.5.c link local

 3.5.d unique local

 3.5.e eui 64

 3.5.f auto-configuration



Computer Addressing - TOC

0. Computer Addressing Format
 1. *Port Address/No., Physical Address {MAC}, Logical Addressing {IPv4 & IPv6}*
1. Binary Octet to Decimal Conversion
2. Binary to Hexadecimal Conversion
3. IPv4 Addressing Basics
 1. *Class*
 2. *Subnet Mask*
 3. *Prefix*
 4. *Network Bits*
 5. *Host Bits*
 6. *No. of Networks*
 7. *No. of Hosts*
 8. *Network Address*
 9. *Broadcast Address*
 10. *Valid Host Addresses Range*
4. Private vs. Public Address
5. CIDR to Subnet Mask Conversion
6. Class C Subnetting
7. Class B Subnetting
8. Class A Subnetting
9. VLSM
10. IPv6 Basics



Computer Addressing Format

Address Types	Port Address	MAC Address	IPv4 Address	IPv6 Address
Definition:	Logical Interface for applications	Packet Forwarding	Routing i.e. Select the best route	Routing i.e. Select the best route

Address	Length {bits}	Divided into	Full Range	Represented	Example
Port Add	16	3 Blocks: 1)0-1023 = Well-Known Ports 2)1024-49,151 = Registered Ports 3)49,152-65,535 = Dynamic or Private Ports	0-65,535	Decimal	HTTP = 80
MAC Add	48	Two 24 bits { OUI & VA} {1 Hexa = 4 bits}	0000-FFFF	12 Hexa Digits	ABCD:1234:AAAA
IPv4 Add	32	4 Octets {1 Octet = 8 bits}	0 to 255	Dotted Decimal Notation	192.168.1.1/24
IPv6 Add	128	8 Groups of 4 Hexa Digits {1 Hexa= 4 bits}	0000-FFFF	32 Hexa Digits	2001:0000:0000:0000:0000:0000:0000:0001/64



Network Layer Protocol :IP version 4

Numbering systems

- Binary {0 & 1} - Machines understand only 0's & 1's
- Octal {0–7}
- Decimal {0-9} – IPv4
- Hexa-decimal {0-9, A{10}, B{11}, C{12}, D{13}, E{14} & F{15}}
 - MAC address & IPv6 Address

• Conversions

- Binary octet[8bits] to Decimal Conversion

$$\begin{array}{cccccccc}
 128 & 64 & 32 & 16 & 8 & 4 & 2 & 1 \\
 \cdot 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
 \cdot 0 + & 64 + & 32 + & 0 + & 8 + & 0 + & 0 + & 1 = 105
 \end{array}$$

- Decimal to Binary octet Conversion
 - 1, 255, 121, 63, 127, 240, 252, 3, 130, 10
- Binary to Hexa Decimal Conversion
- Hexa Decimal to Binary Conversion
 - 0123:4567:89AB:CDEF



Network Layer Protocol :IP version 4

- Internet Protocol version 4
- 32 bit address
- Divided in to 4 octets {1 octet = 8 bits}
- For Easy representation
 - Converted into Dotted decimal notation
 - 192.168.1.1
- Full range
 - 0.0.0.0 – 255.255.255.255
- Class {In First Octet}
 - >Hosts
 - A [1-126] – 1.0.0.0 – 126.255.255.255
 - B [128-191] – 128.0.0.0 – 191.255.255.255
 - C [192-223] – 192.0.0.0 – 223.255.255.255
 - >Reserved:
 - D [224-239] – 224.0.0.0 – 239.255.255.255 – Reserved for Multicast
 - E [240-254] – 240.0.0.0 – 254.255.255.254 – Reserved for R&D labs

Network Layer Protocol :IP version 4

- Subnet Mask

- 32 bit address –represented in dotted decimal notation
- Purpose: To identify the Network bits{NID} & Host bits{HID} in the IP Address.
 - IP : 192.168.1.1 {32 bits}
 - SM : 255.255.255.0
 - Address
 - Network Address = Area Address {JP Nagar}
 - Host Address = Street Address {2nd street}
 - MAC Address = Door No. {16}
 - All 1's are Network bits
 - All 0's are Host bits
 - N.N.N.H = 24 Network bits & 8 host bits

- Default subnet mask Prefix{/network bits} i.e. 192.168.1.1/24

- A – 255.0.0.0 /8
- B – 255.255.0.0 /16
- C – 255.255.255.0 /24



Network Layer Protocol :IP version 4

- Reserved IP Addresses

- 127.x.x.x = Loopback address - for self testing of L4, L3, L2 & L1
 - CMD>ping 127.0.0.1 to 127.255.255.254
- 169.254.0.1 through 169.254.255.254 – for self-configured IP address
 - APIPA – Automatic Private IP Address
- In every NW, we reserved 2 addresses
 - Network Address: In IP, host bits(HID) all 0's
 - Broadcast Address: In IP, host bits (HID) all 1's
 - Example: IP : 192.168.1.1 /24 i.e. N.N.N.H
 - NA: 192.168.1.0
 - BA: 192.168.1.255
 - First Host Address[NA+1]:192.168.1.1
 - Last Host Address[BA-1]: 192.168.1.254

$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16$
$2^5 = 32$
$2^6 = 64$
$2^7 = 128$
$2^8 = 256$
$2^9 = 512$
$2^{10} = 1024$
$2^{11} = 2048$
$2^{12} = 4096$
$2^{16} = 65K$
$2^{24} = 16M$

- No of Networks

- $2^n \text{ } n=\text{network bits} = 2^{24} = 16M$

- No of Hosts

- $2^n - 2 \text{ } n=\text{host bits} = 2^8 - 2 = 256 - 2 = 254$



IPv4 Basic Exercise

- **192.168.1.1**

- | | |
|------------------------------|---|
| 1. Class | : |
| 2. Default Subnet mask | : |
| 3. Prefix | : |
| 4. No. of Network bits | : |
| 5. No. of Host bits | : |
| 6. No. of Networks | : |
| 7. No. of Hosts | : |
| 8. Network Address | : |
| 9. Broadcast Address | : |
| 10. Valid Host Address range | |
| 10.1 First host address | : |
| 10.2 Last host address | : |

Exercise Questions:

- 1) **7.6.5.4**
- 2) **130.130.1.222**
- 3) **221.220.219.218**
- 4) **127.0.1.2**
- 5) **17.16.7.0**



Network Layer Protocol :IP version 4

Full Range:

Class	Subnet Mask decimal	No. of Hosts per Network	No. of Networks	Start - End Address
A	255.0.0.0	16 Million	127	1.0.0.0 - 126.255.255.255
B	255.255.0.0	65000	16000	128.0.0.0 - 191.255.255.255
C	255.255.255.0	254	2 Million	192.0.0.0 - 223.255.255.255
D	Reserved for multicast groups			224.0.0.0 - 239.255.255.255
	Reserved for future use, or Research and Development Purposes			
E	Development Purposes			240.0.0.0 - 254.255.255.254

N.H.H.H
N.N.H.H
N.N.N.H

Private IP Address Range:

Class	Address Range	Default Subnet
A	10.0.0.0 -> 10.255.255.255	255.0.0.0
B	172.16.0.0 -> 172.31.255.255	255.255.0.0
C	192.168.0.0 -> 192.168.255.255	255.255.255.0

Classless Inter Domain Routing {CIDR} to subnet mask conversion:

>>>Practice: /0 to /32



IPv4 :Class C Sub netting

- Scenario: 192.168.1.0/24 Need: 3 subnets

1. Public/Private Address :
2. CIDR: /n { n = Number of Network bits}[N+S]:
3. Subnet Mask :
4. No. of Subnets: 2^n :
- * n = Number of Sub network bits {S}
5. No. of Hosts per each subnet : $2^n - 2$
* n = Number of Hosts bits {H}
6. Magic Number or Multiplier :
7. 1st subnet Network Address :
8. 1st subnet Broadcast Address :
9. Last subnet Network Address :
10. Last subnet Broadcast Address :
11. Full Subnets Range Table: {Min 1st three subnets & Last 3subnets}
12. Breakup for Hosts addresses in the 1st subnet:

Exercise Questions:

- 1) 192.168.4.0/24 Need: 50 subnets
- 2) 192.168.3.0/24 Need: 9 networks
- 3) 192.168.2.0/24 Need: 63 subnets
- 4) 192.168.1.0/24 Need: 31 hosts
- 5) 192.168.254.0/24 Need: 7 computers

Full Range Table [FRT]

Subnet	Network Address	1 st Host Address	Last Host Address	Broadcast Address
1 st Subnet				
2 nd Subnet				
3 rd Subnet				
Last Subnet				



IPv4 :Class B Sub netting

- **172.15.0.0/16 Need: 100 Networks**

1. Public/Private Address:
2. CIDR: /n { n = Number of Network bits} {N+S}
3. Subnet Mask:
4. No. of Subnets: 2^n
 * n = Number of Sub network bits {S}
5. No. of Hosts in each subnet: $2^n - 2$
 * n = Number of Hosts bits {H}
6. Magic Number or Multiplier:
7. 1st subnet Network Address:
8. 1st subnet Broadcast Address:
9. Last subnet Network Address:
10. Last subnet Broadcast Address:
11. Full Subnets Range Table: {Min 1st three subnets & Last 3subnets}
12. Breakup for Hosts addresses in the 1st subnet:

Exercise Questions:

- 1) **172.32.0.0/16 Need:200 Hosts**
- 2) **165.11.0.0/16 Need: 16 subnets**
- 3) **179.50.0.0/16 Need: 2000 computers**
- 4) **190.81.0.0/16 Need: 50 computers**

Subnet	Network Address	1 st Host Address	Last Host Address	Broadcast Address
1 st Subnet				
2 nd Subnet				
3 rd Subnet				
Last Subnet				



IPv4:Class A Sub netting

- **6.0.0.0/8 Need=3200 Computers/Hosts**

1. Public/Private Address:
2. CIDR: /n { n = Number of Network bits} {N+S}
3. Subnet Mask:
4. No. of Subnets: 2^n
 * n = Number of Sub network bits {S}
5. No. of Hosts in each subnet: $2^n - 2$
 *n = Number of Hosts bits {H}
6. Magic Number or Multiplier:
7. 1st subnet Network Address:
8. 1st subnet Broadcast Address:
9. Last subnet Network Address:
10. Last subnet Broadcast Address:
11. Full Subnets Range Table: {Min 1st three subnets & Last 3subnets}
12. Breakup for Hosts addresses in the 1st subnet:

Exercise Questions:

1) 6.0.0.0/8 Need=3200 Subnets

Subnet	Network Address	1 st Host Address	Last Host Address	Broadcast Address
1 st Subnet				
2 nd Subnet				
3 rd Subnet				
Last Subnet				



CIDR/VLSM

- Variable Length Subnet Mask{VLSM}

Key Concept: *Variable Length Subnet Masking (VLSM) is a technique where subnetting is performed multiple times in iteration, to allow a network to be divided into a hierarchy of subnetworks that vary in size. This allows an organization to much better match the size of its subnets to the requirements of its networks.*

- Classless Inter Domain Routing {CIDR}

- Super-netting, also called Classless Inter-Domain Routing ([CIDR](#)), is a way to aggregate multiple Internet addresses of the same class.

Reference Links:

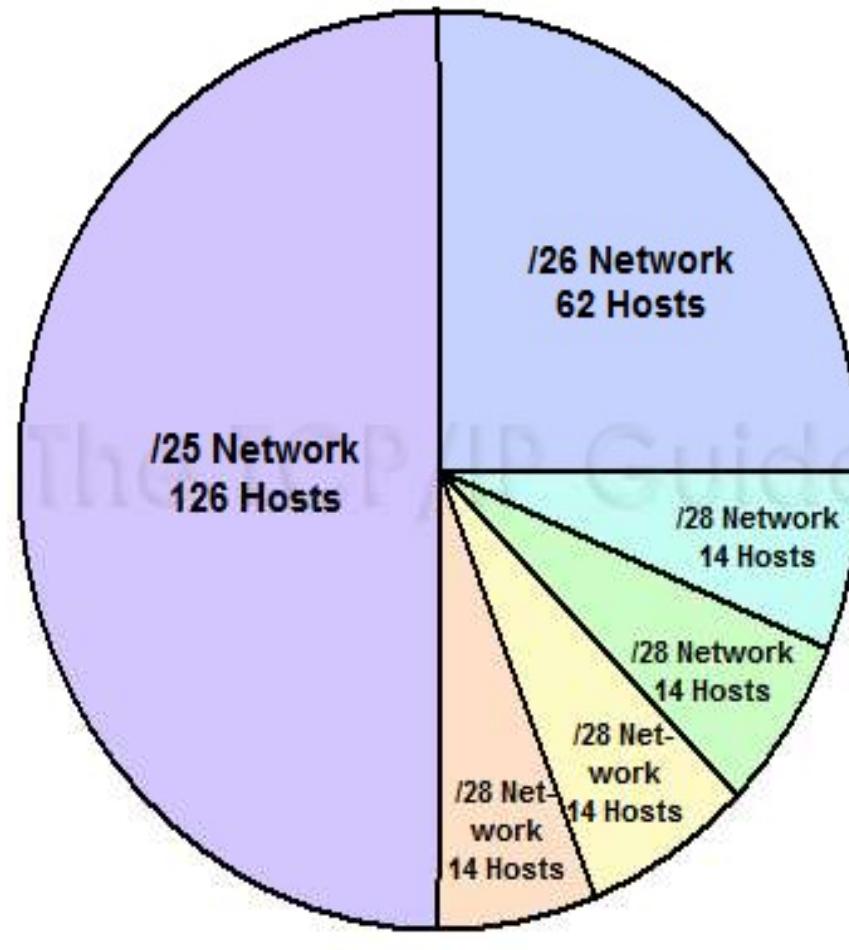
<http://searchnetworking.techtarget.com/definition/supernetting>

http://www.tcpipguide.com/free/t_IPVariableLengthSubnetMaskingVLSM-2.htm



CIDR/VLSM

VLSM – Variable Length Subnet Mask



Class C (/24) Network (254 Hosts)

Classless inter domain routing
CIDR or Super netting

$192.168.1.0/24 = 254 \text{ hosts}$
 $192.168.1.0/23 = 510 \text{ hosts}$

NA: 192.168.1.0/24

Need:
6 Networks/Subnets
1 NW = 100 Hosts
2 NW = 50 Hosts
3 NW = 10 Hosts
4 NW = 11 Hosts
5 NW = 12 Hosts
6 NW = 9 Hosts

CIDR/VLSM

VLSM – Variable Length Subnet Mask

Variable Length Subnet Masking [VLSM]							
Need hosts	Subnet ID	Network Address/CIDR	1st Host Address NA+1	Last Host Address BA-1	Broadcast Address Next Subnet NNA-1	Magic Number	No. of Hosts
100	1	192.168.1.0/25	192.168.1.1	192.168.1.126	192.168.1.127	128 {4th OCT}	126
50	2	192.168.1.128/26	192.168.1.129	192.168.1.190	192.168.1.191	64 {4th OCT}	62
10	3	192.168.1.192/28	192.168.1.193	192.168.1.206	192.168.1.207	16 {4th OCT}	14
11	4	192.168.1.208/28	192.168.1.209	192.168.1.222	192.168.1.223	16 {4th OCT}	14
13	5	192.168.1.224/28	192.168.1.225	192.168.1.238	192.168.1.239	16 {4th OCT}	14
9	6	192.168.1.240/28	192.168.1.241	192.168.1.254	192.168.1.255	16 {4th OCT}	14



Network Fundamentals

IPv6 Addressing

Lesson 24



IPv6 : Table of Contents

1. IPv6 Addressing

1. IPv6 Addressing Format
2. IPv6 Headers & Address Types
3. In Depth Exploration: understanding the New address

2. IPv6 Configuration

1. Assigning IPv6 Address to your Router
2. Routing IPv6 – Static & OSPFv3

3. IPv4 – IPv6 Migration Strategies



- Will we ever need to upgrade to IPv6 ?

Rationale for IPv6:

- Yes, there is an IP address Shortage
- Current IP addresses poorly Allocated
- New network devices on the rise
- NAT {our current solution} is now seen a Hindrance to Innovation
- Potential Features:
 - IPSEC Everywhere, i.e. VPN connections & Encryption
 - Mobility,
 - Simpler header

IPv6 – Addressing Format

IP Addressing:

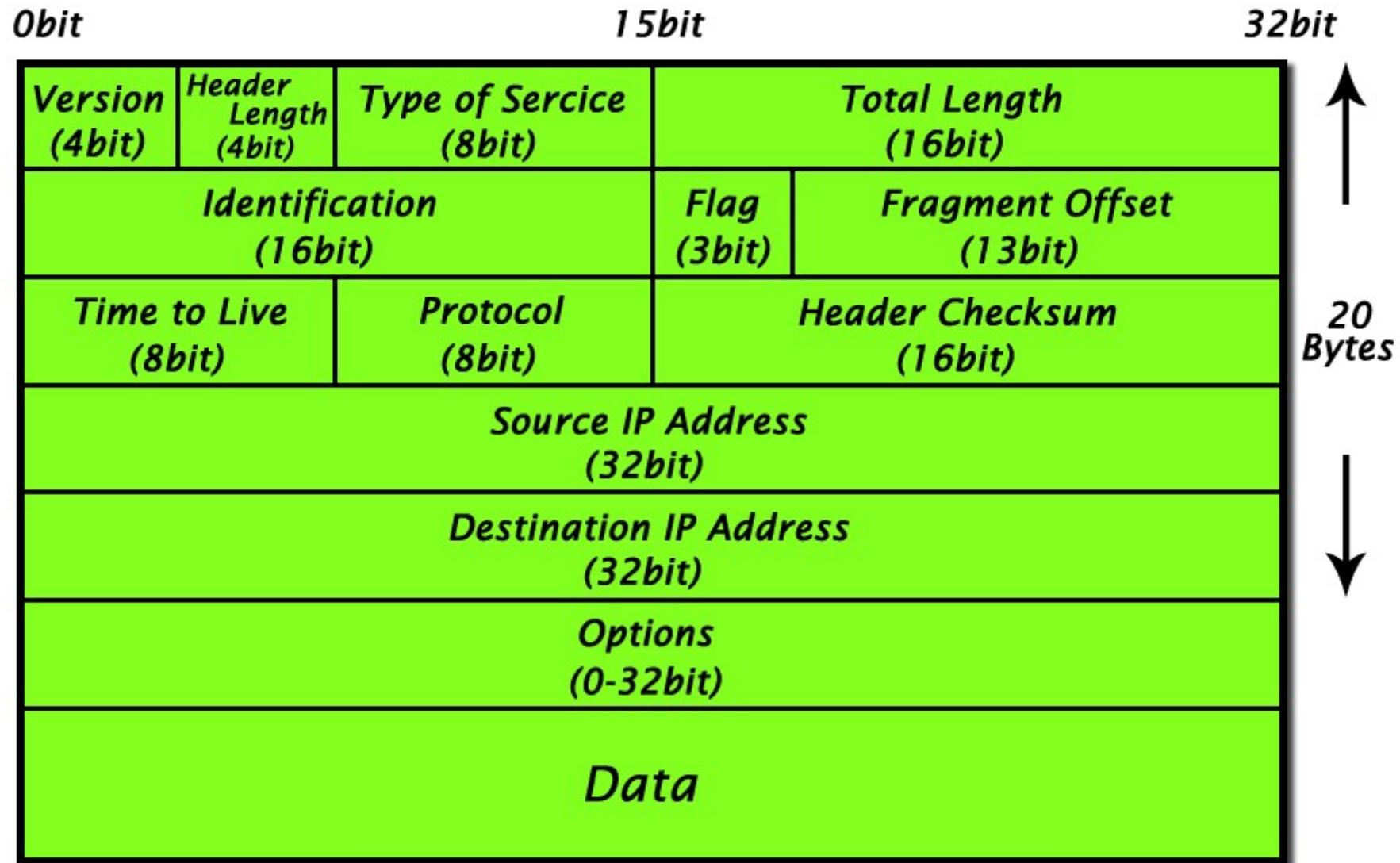
- 32 bits {IPv4} to 128 bits {IPv6}
- Provides 340, 282, 366,920,938,463,463,374, 607,431, 770,000...0000
 - 340 undecillion IP addresses
 - 3.4×10^{38}
 - *So we could assign an IPV6 address to EVERY ATOM ON THE SURFACE OF THE EARTH,*
- To make Address more manageable, Divided into 8 groups of 4 Hex characters
 - 2001:0050:0000:0000:0000:0AB4:1E28:98AA
 - Rule 1: Eliminate Groups of Consecutive zeros
 - 2001:0050::0AB4:1E28:98AA
 - Rule 2: Drop Leading zero i.e. No Trailing zeros
 - 2001:50::AB4:1E28:98AA

<http://itknowledgeexchange.techtarget.com/whatis/ipv6-addresses-how-many-is-that-in-numbers/>



	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	$2^{32} = 4,294,967,296$	$2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456$

IPv4 Header Format



IPv6 Header Format

<i>Version</i>	<i>Traffic Class</i>	<i>Flow Label</i>	
	<i>Payload Length</i>	<i>Next Header</i>	<i>Hop Limit</i>
<i>Source Address</i>			
<i>Destination Address</i>			

IPv6 Addresses

Types of communication and address:

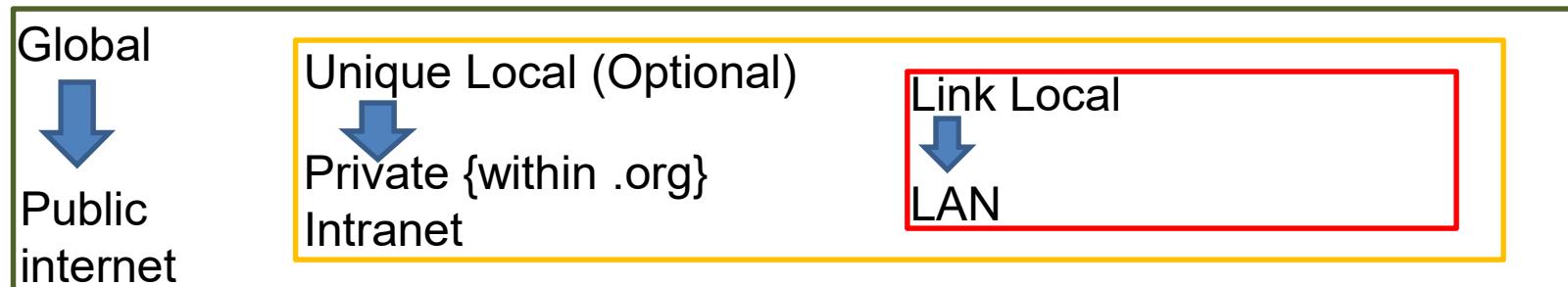
IP addresses by IANA – Internet Assigned Numbers Authority

➤ CASTING:

- Unicast : one - To – one
- Multicast: one – To – Many
- Anycast: one - To – Closest {LAN}

➤ Addresses:

- Link Local Scope Address: Layer 2 Domain
- Unique/Site. Local Scope Address: Organization {Private}
- Global Scope Address: Internet {Public}



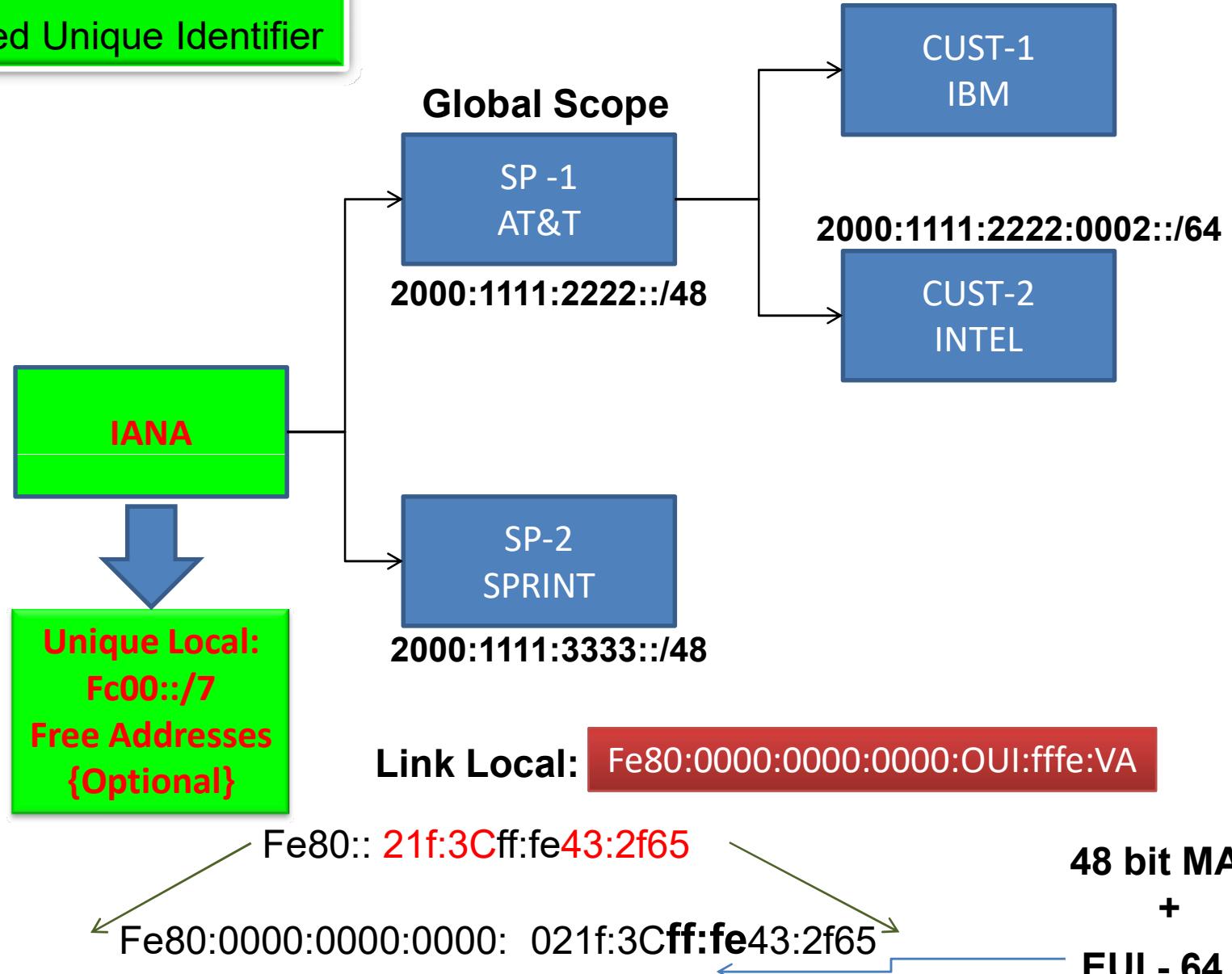
<http://itknowledgeexchange.techtarget.com/whatis/ipv6-addresses-how-many-is-that-in-numbers/>



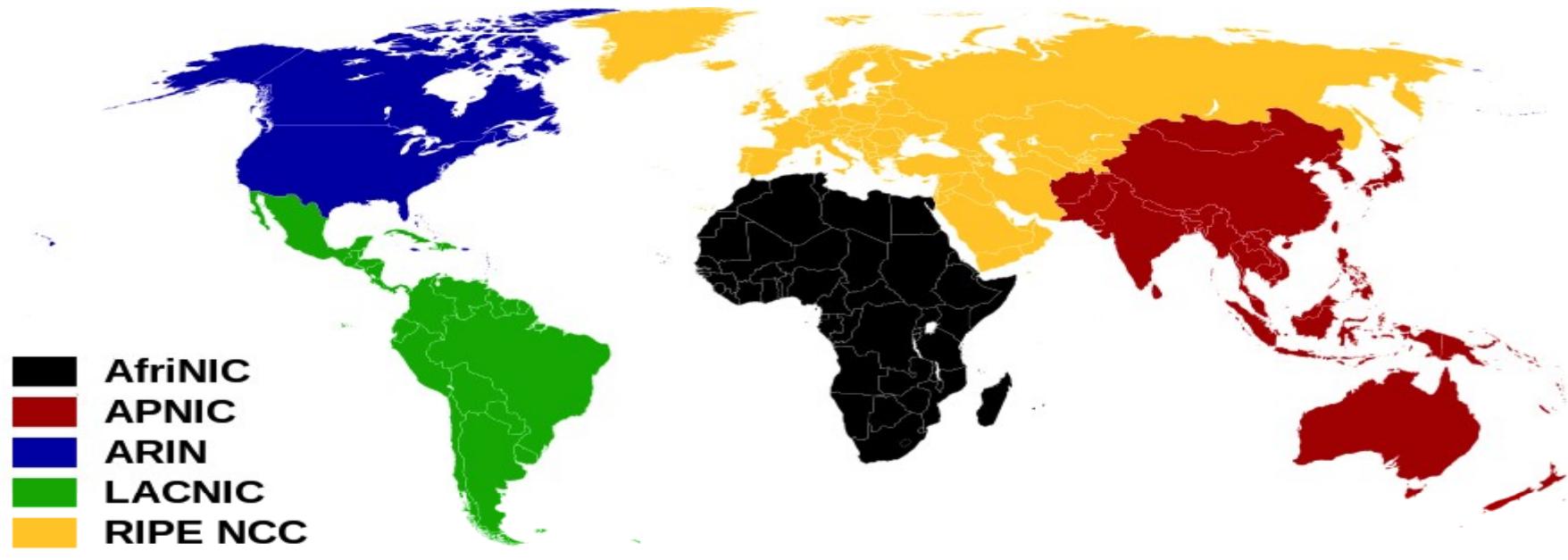
IPv6 Addressing

2000:1111:2222:0001::/64

Legend:
EUI-Extended Unique Identifier



Bye IPv4 & Hello IPv6



Type	Binary	Hex
Aggregatable Global Unicast	001	2000::/3
Link-Local Unicast	1111 1110 10	FE80::/10
Unique Local Unicast	1111 1100	FC00::/8
	1111 1101	FD00::/8
Multicast	1111 1111	FF00::/8

<https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml>



kumar6009@gmail.com



@air.ds2

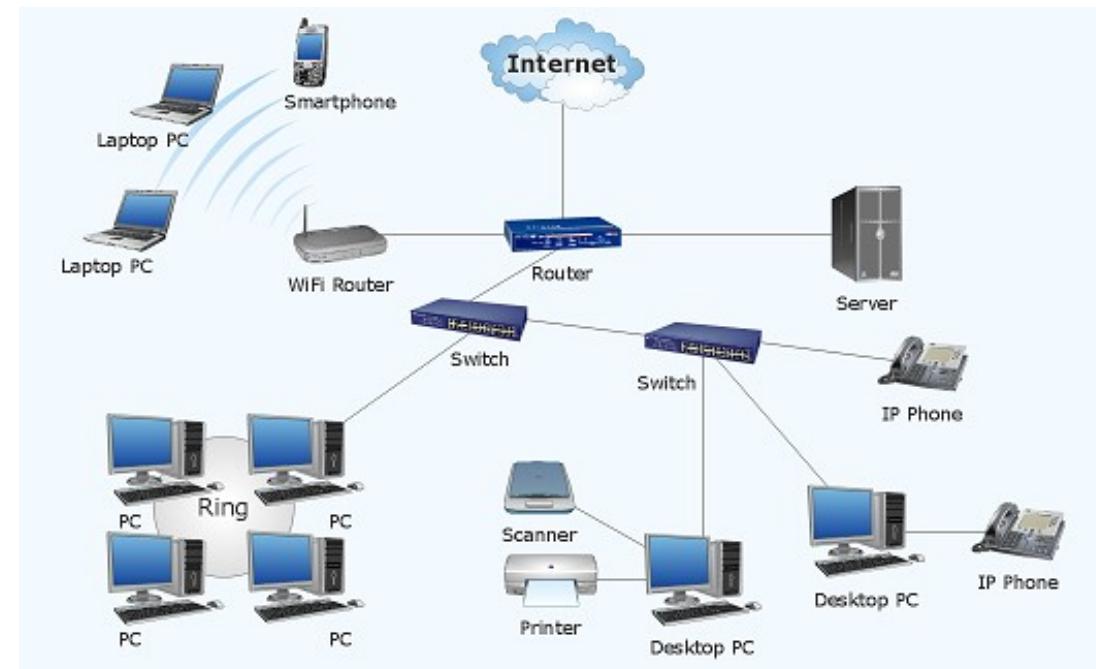
Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3 118

LAN Switching Technologies

Network Devices

Purpose & Functions



Network devices : Purpose & Functions

1. NIC i.e. Network Interface Card
2. Repeater
3. Hub
4. Bridge
5. Switch
6. Router
7. BD/CD Exercise

Purpose & functions of network devices

➤ What is a Network?

- Computer Network: Collection of autonomous computers interconnected by a single/same technology
- Benefits:
 - Able to exchange information {Data}
 - Share Resources [Devices or Services]

➤ Types of Network?

1. Peer – to - Peer Network i.e. within two computers - Ethernet
2. Local Area Network {LAN} i.e. within single building premises
3. Campus Area Network {CAN} i.e. within a campus
4. Metropolitan Area Network {MAN} i.e. within a city
5. Wide Area Network i.e. WAN
 1. Intranet[same], Extranet[diff.] & Public {Internet}
 1. Inter city/state/country connectivity
 2. Inter planet – Earth to mars – satellite technology

Purpose & functions of network devices

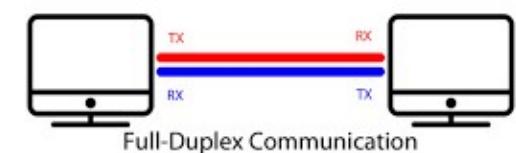
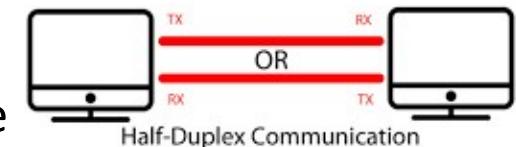
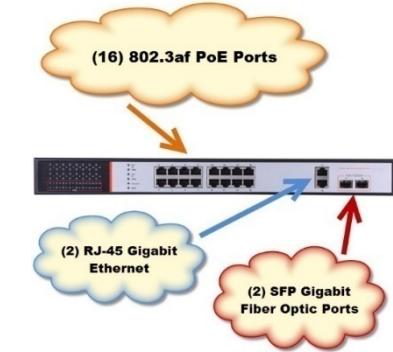
- Network Interface Card
 - Every network device must have a NIC
 - Address:
 - Physical Address i.e. Forwarding/Switching
 - Unique Address i.e. LAN > Ethernet > MAC Address [OUI+VA]
 - Hard coded by vendor in the chipset itself
 - Logical Address i.e. Routing
 - IP address will be configured by admin i.e. IPv4, IPv6
 - Connects in the Motherboard of a device {PC}
- Repeater
 - Purpose:
 - Every Media has a Distance Limitation
 - To overcome the distance limitation, we use Repeater
 - Function
 - Voltage Amplifier
 - 5-4-3 Rule
 - 5= Segments , 4=Repeaters & 3=Populated Segments

Purpose & functions of network devices

- Hub
 - Multi port Repeater
- What is a topology?
 - Physical [wire] Map of a Network
 - To understand the data flow between hosts i.e. PC's, servers, routers & switches
- Types of topology?
 1. Bus Topology
 2. Ring Topology
 3. Star Topology
 4. Hybrid Topology
 5. Mesh Topology
 6. Point –to –point
 7. Point – to -Multipoint

Purpose & functions of network devices

- Bridge
 - Different technology/topology connector
 - Now-a-days repeater, Hub, Bridge devices are not used.
 - But the concepts are used in switching.
- Switching Terminologies
 - Transmission Methods:
 - Unicast: 1 to 1
 - Multicast: 1 to many/group
 - Broadcast: 1 to All
 - Communication Modes:
 - Simplex {One way communication}
 - Duplex {Two way communication}
 - » Half Duplex {Only one side at a time – i.e. Transmit/Receive – Ex: Walky – Talky}
 - » Full Duplex {Both side at a time – i.e. Transmit/Receive – Ex: Telephone call}
 - [CSMA/CD & CSMA/CA] [to reduce the collisions on network]
 - Carrier sense Multiple access/ Collision Detection
 - Carrier sense Multiple access/ Collision Avoidance
 - What is Broadcast Domain?
 - What is Collision Domain?



Purpose & functions of network devices

– CSMA/CD

1. PC must have data to send
2. It senses the carrier
3. If carrier is free
4. PC will send data
5. While sending the PC will monitoring for data fragmentation {collision}, if collision detects, request for retransmission

– CSMA/CA

1. PC must have data to send
2. It senses the carrier
3. If carrier is free
4. PC will send the JAM signal
5. Wait for other PC's to process JAM signal
6. PC will send data
7. If other PC's want to send data, the carrier will be shared on time basis

Purpose & functions of network devices

– What is Collision?

- If 2 PC's sends data at same time in the single/same media, the data get hit and fragmented {Damaged}. This is called Collision

– What is Domain?

- Single Administrative area
 - Group of Hosts{PC} with same set of rules/policies

– What is Broadcast Domain?

- If a PC sends a Broadcast data, till what area the data can flow in the network, that complete area is called as single broadcast domain

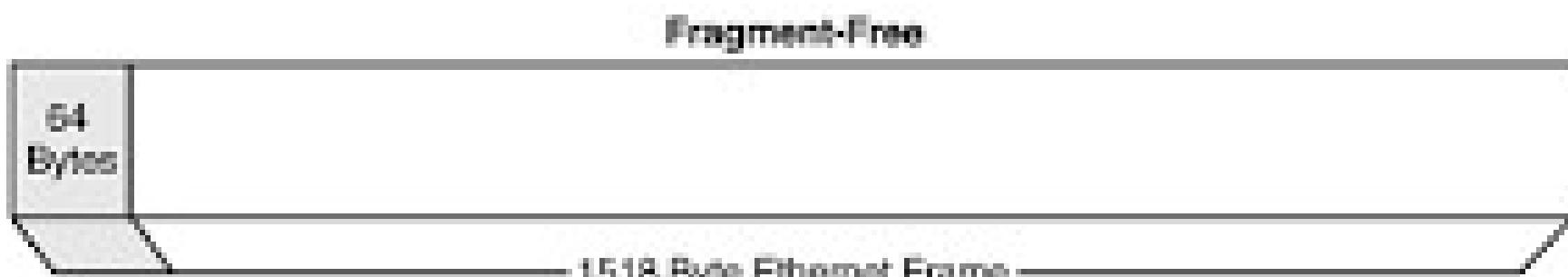
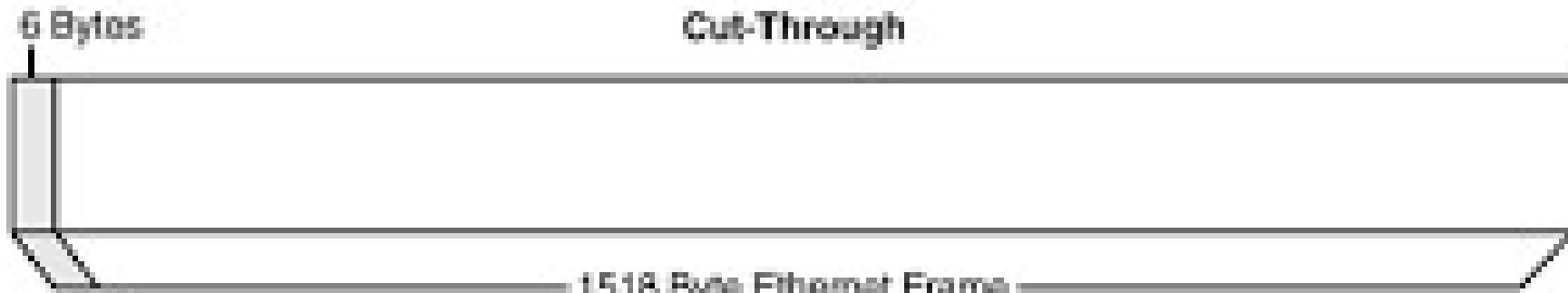
– What is Collision Domain?

- If 2 PC's sends data at a same time, till what area the data may get hit and collision will happen in the network, that complete area is called as single collision domain

Purpose & functions of network devices

- Switch
 - Purpose:
 - Collision free network
 - Fast wire speed network
 - Hub : 10mbps
 - Switch: 100mbps, 1Gbps, 10Gbps, 40Gbps, 100Gbps etc....
 - Function:
 - Breaking the single collision domain & making every port as a separate single collision domain i.e. Switching Fabric
 - Active device
 - Intelligent device
 - CPU & RAM
 - » RAM : CAM table – Content Addressable Memory table
 - » CAM : Switch Port no. & Source MAC Address
 - Single Broad cast domain
 - Multiple Collision Domain

Purpose & functions of network devices



Purpose & functions of network devices

Router

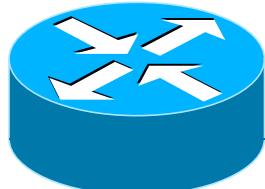
- Purpose
 - LAN-WAN Connector
 - Connects different logical networks i.e. Subnets
- Function
 - Route Lookup
 1. Select the best the path i.e. static (manually) & Dynamic (auto - using routing protocols)
 2. Put best route info(Destination NA: Next hop ip /exit interface) to the routing table of the router
 - Forward Lookup
 1. Find the Next hop IP's MAC using ARP
 - ARP Protocol is used to find MAC Address using IP address by ARP broadcasts
 - Update the ARP table in router i.e. 10.1.12.2 = 2222
 2. Frame Rewrite i.e. Change Source MAC & Destination MAC
 3. Forward the packet in the exit interface
 - By default, Router Blocks Broadcast Packets
 - Breakup Broadcast Domain {M BD}
 - Breakup collision Domain {using ARP table -MCD }

Devices	BD	CD
Repeater/Hub	1	1
Bridge/Switch	1	Multiple
Router	Multiple	Multiple

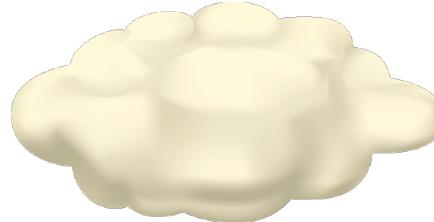


Purpose & functions of network devices

- Symbols i.e. Cisco Icons



Router 



Cloud - Internet

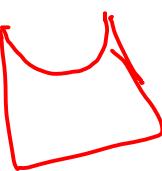


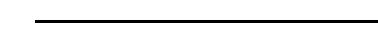
Switch 



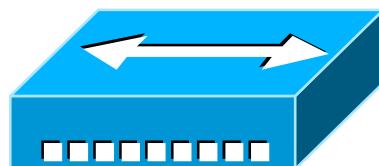
WAN - Serial

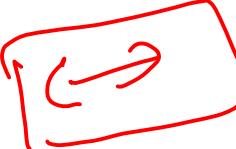


Bridge 

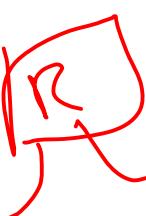


LAN - Ethernet

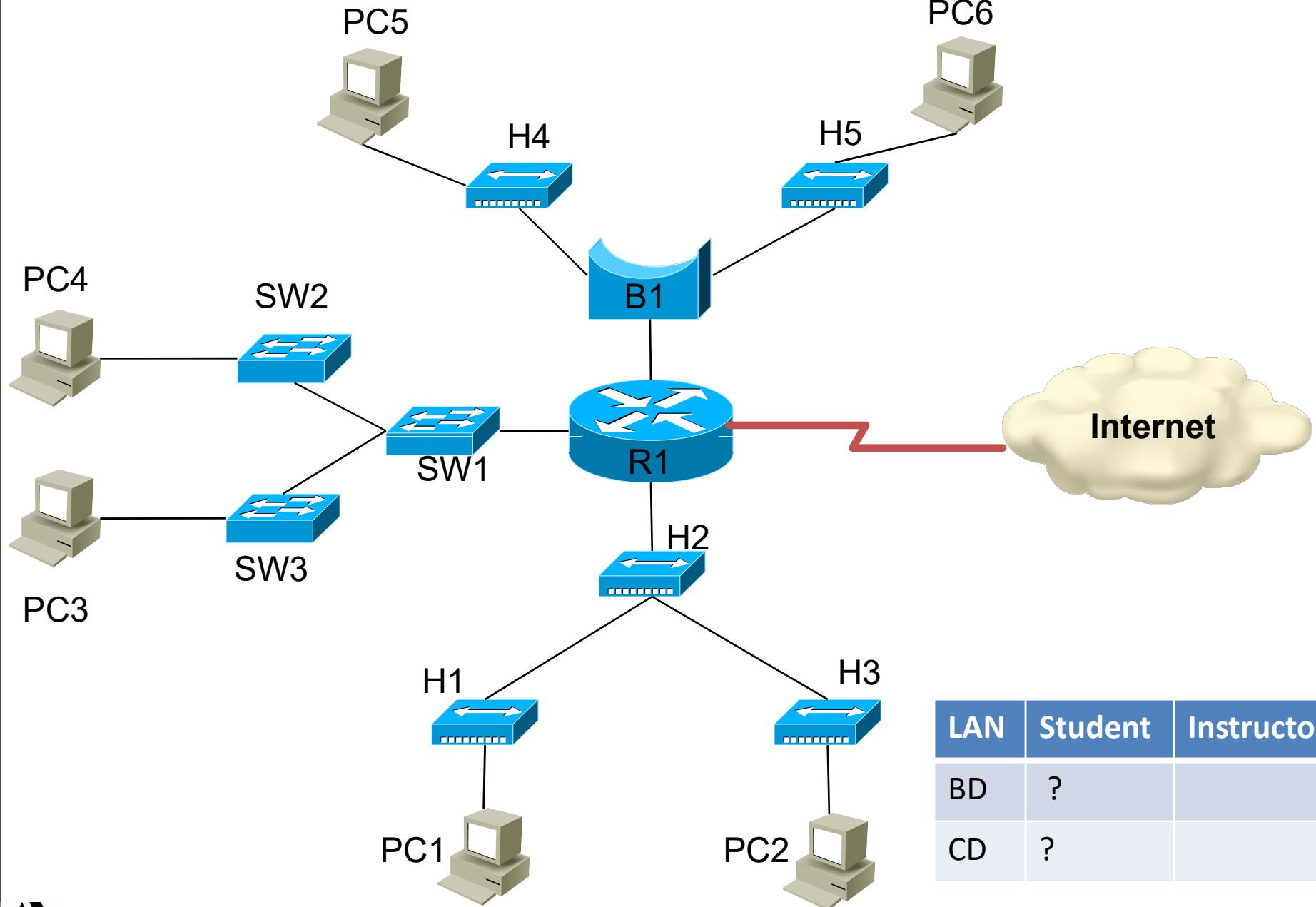


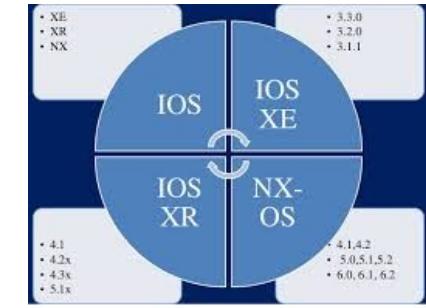
Hub 



Repeater 

Broadcast Domain & Collision Domain Exercise





LAN Switching Technologies

IOS Basics

Lesson 26



Lines i.e. Login Methods

Login into a Device {Lines:}

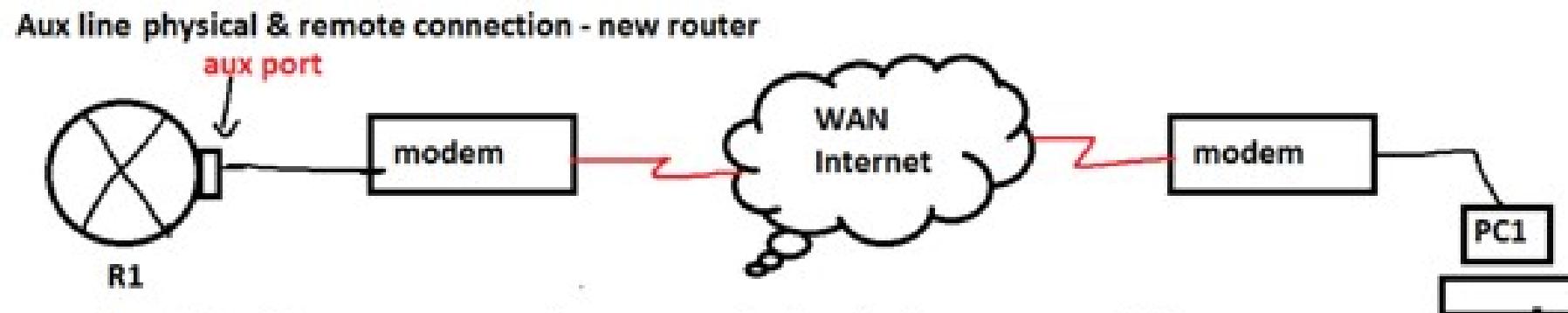
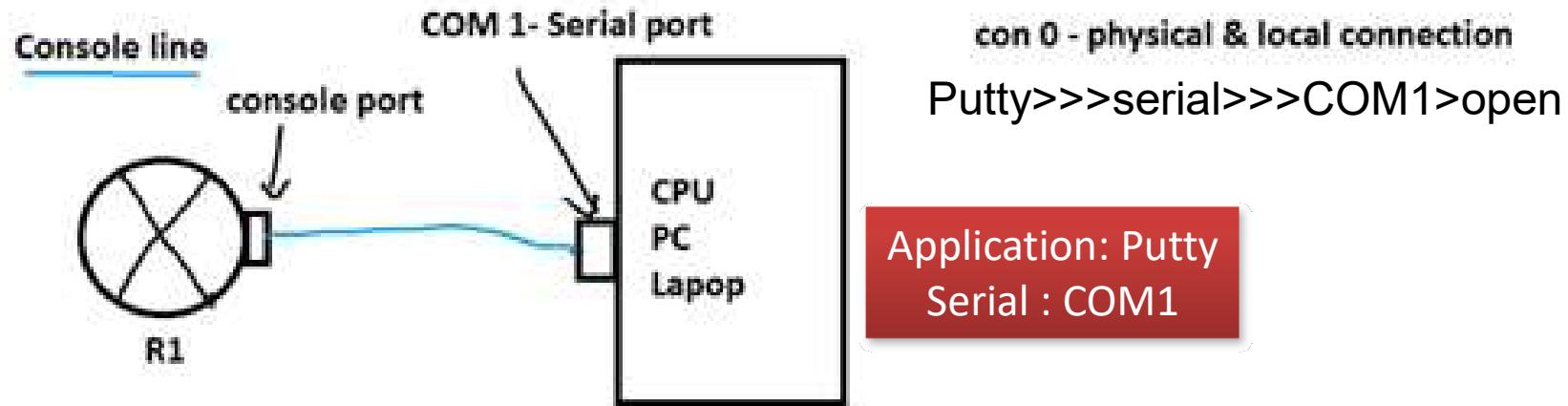
1. CONSOLE [CTY]
 - Physical & Local Connection
2. AUX [Auxiliary Line]
 - Physical & Remote Connection via Modem
3. VTY – Virtual Terminal
 - Virtual & Remote Connection
 - any LAN/WAN interface, ip add, line psswd
 - Protocols i.e. Telnet(plain text) & SSH(Cipher Text)
4. TTY - Terminal Controller
 - Virtual & Remote Connection
 - Specialized devices – i.e. For Access Server Login
5. HTTP/HTTPS
 - Web {Remote Connection}
6. x/y/z
 - Slot/Sub slot/Port

➤ Console Line:

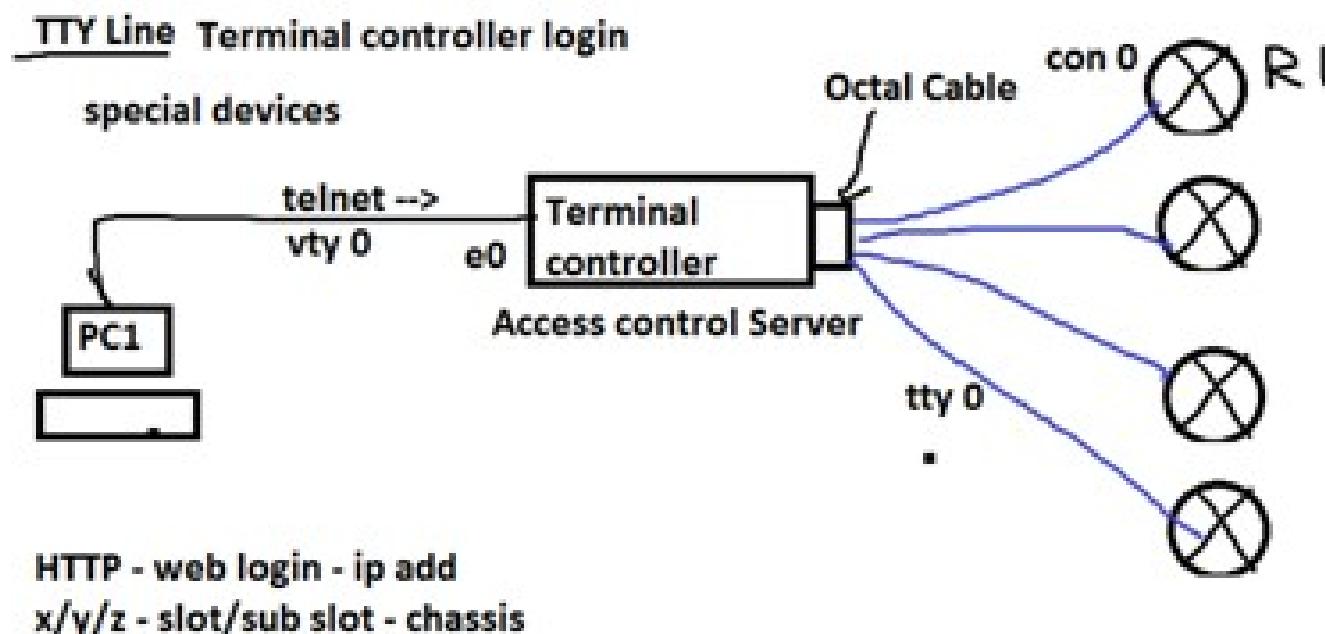
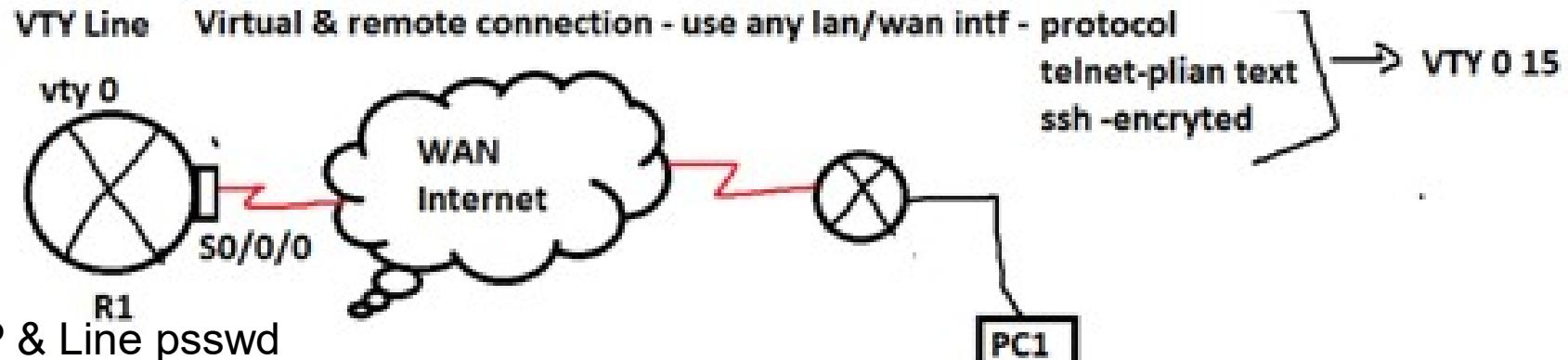
- Software:
 - Windows XP: Hyper Terminal
 - Other systems: Putty
- Cable & Converters:
 - Console cable i.e. RJ45 to RS232



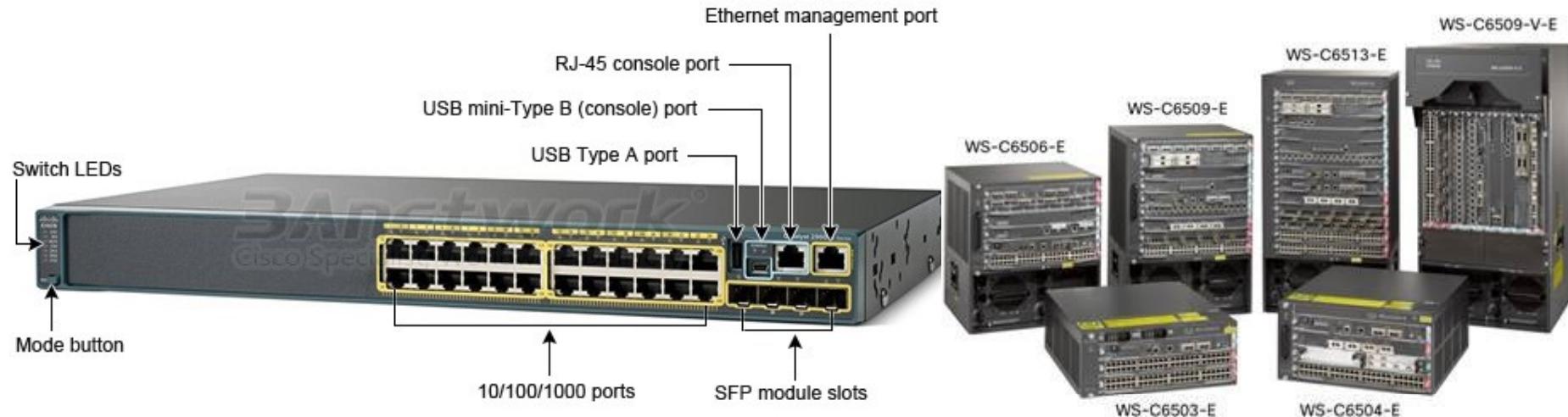
Login Methods



Login Methods



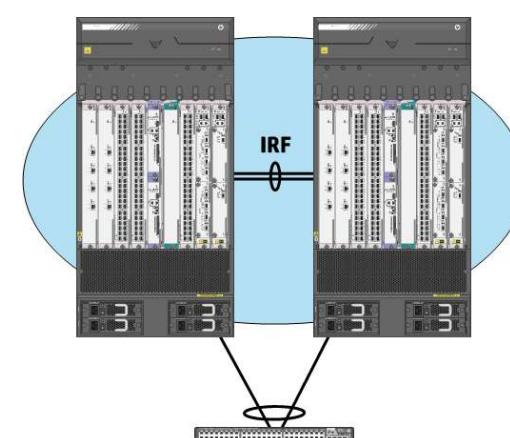
Switch Configuration - Interfaces



Stacking – virtual – 1 SW



Chassis aggregation/virtualization



VSS is Cisco, IRF is HP.

Virtual Switching Systems (VSS)

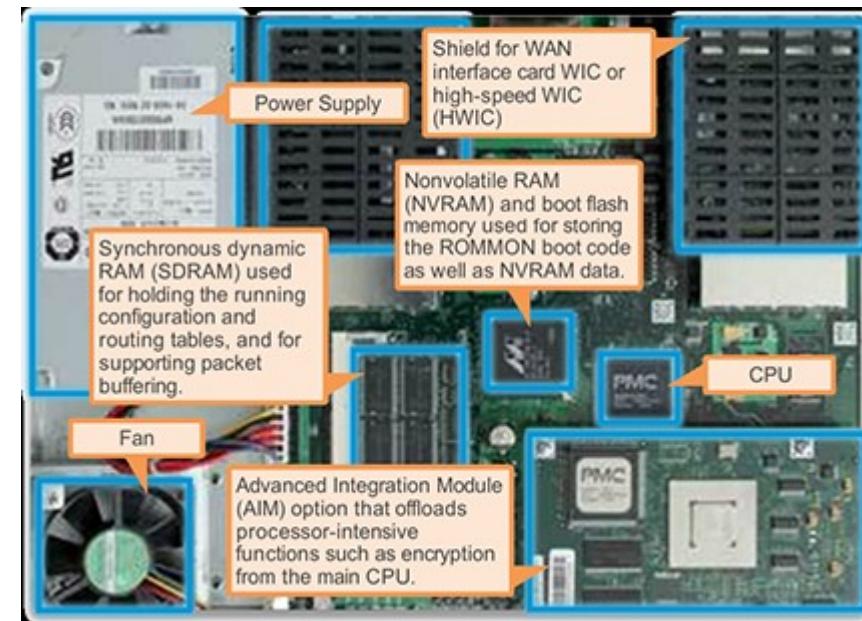
Intelligent Resilient Framework (IRF)

Hardware – Block Diagram

RAM	ex: Hard disk	ex: USB drive	FLASH	ROM
Running-config	NVRAM		IOS .bin format	POST Bootstrap program >ROM Monitor mode >Rx Boot mode
	Startup-config			
	CONSOLE	INTERFACES LAN: e0, fa0/0, gig0/0		
	AUX	WAN: S0/0/0, E1/T1		

Router Boot Process:

1. Power-on
2. ROM-Bootstrap program - POST
3. Find IOS
4. IOS is stored in Flash in .bin file
5. Decompress & load in RAM
6. Copy Startup-config from NVRAM(HDD) and
7. Load in RAM i.e. Running-config
8. Router>



Legend:

RAM : Random Access Memory
 ROM: Read Only Memory
 NVRAM: Non Volatile Memory
 FLASH : EEPROM – Electrically Erasable Programmable ROM
 POST: Power on Self Test
 IOS: Internetworking Operating System

Cisco IOS Modes

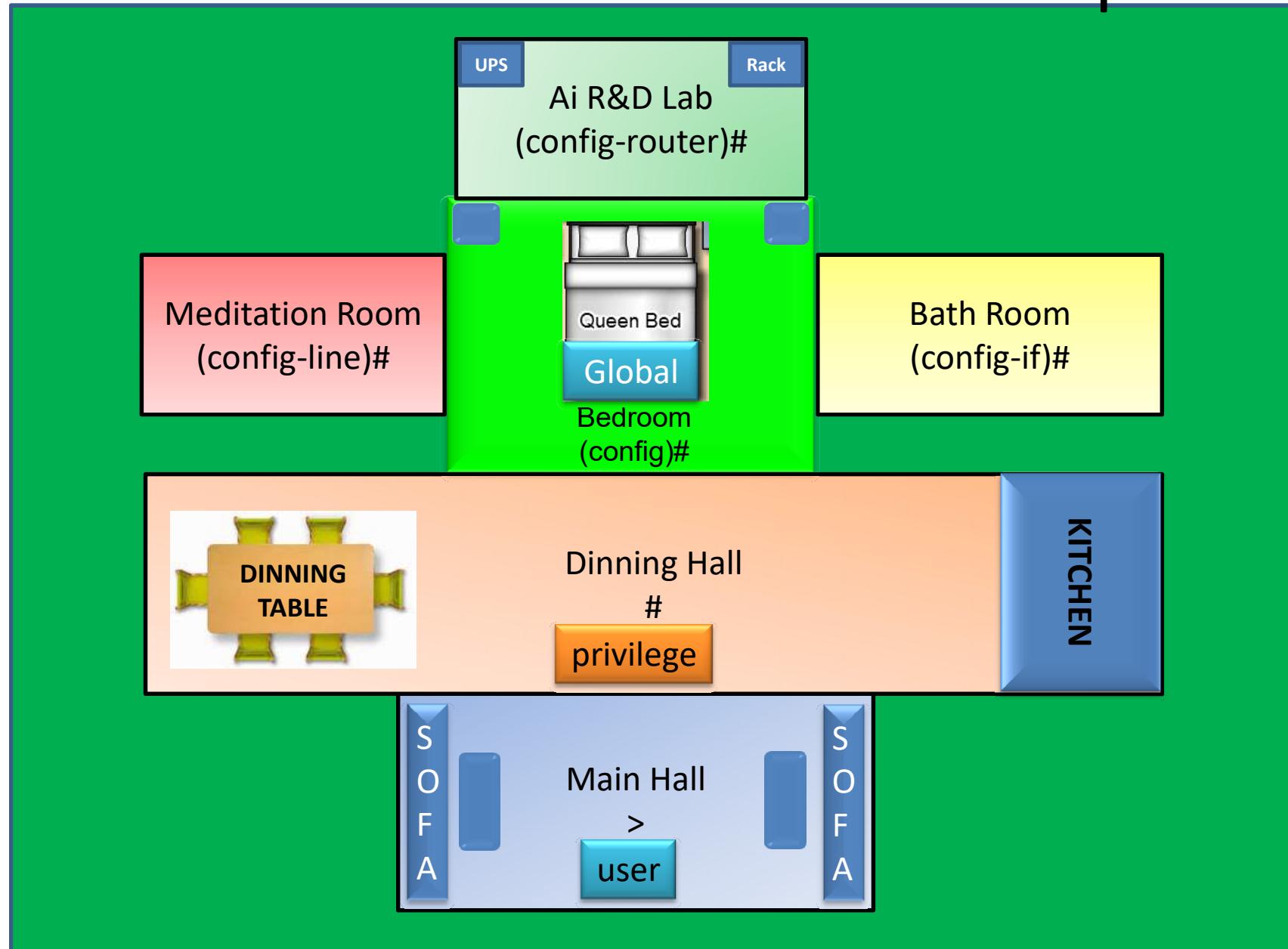
Types of OS : CLI Based OS & GUI Based OS

IOS command Syntax: LHS=Host Name(mode symbol) RHS: commands

S/N	Modes	Description	Mode Symbol	Function	Commands
1	User	User executable mode	>	Min. examination (L1)	By Default
2	Privilege	Privilege Executable mode	#	Max. examination (L2, L3)	>enable
3	Global	Global configuration mode	(config)#	Change settings	#configure terminal
4	Other - Line	Line configuration mode	(config-line)#	console, aux, vty	(config)#line con 0
5	Other-Interface	Interface configuration mode	(config-if)#	fa0/0, s0/0/0	(config)#int fa0/0
6	Other-Router	Router configuration mode	(config-router)#	Routing Protocols: RIP, EIGRP, OSPF, BGP	(config)#router rip
7	RX Boot	RX-Boot / ROM Monitor Mode	ROMMON>	Password recovery, IOS Troubleshooting	Reset & Press Ctrl + C
8	Setup	Setup/Intial configuration mode	[yes/no]:	New router/ No startup-config	No [By Default]

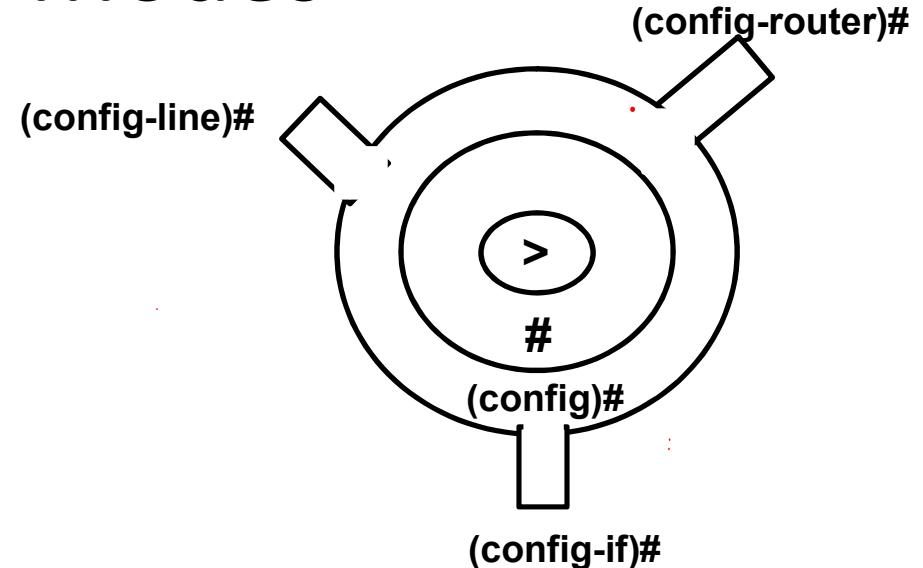


Cisco IOS Modes – Home Example



Cisco IOS Modes

- **User exec mode:**
 - Minimal Examination of SWITCH
 - No changes will takes place
 - SWITCH> Show running-config
 - SWITCH> Show ?
- **Privilege exec mode:**
 - Detail Examination of SWITCH
 - No changes will takes place
 - SWITCH# Show ?
 - .
 - .
 - .
 - .
 -more.... Space bar Page by Page
 -more.... Enter Line by Line
- **Global configuration mode:**
 - SWITCH Configuration i.e. Changing Settings
 - SWITCH(config)#Hostname cisco
 - cisco(config)#



Cisco IOS Modes

- **Other Configuration Mode**
 - **SWITCH(config-if)#**
 - To configure Interfaces {Fa 0/0, S 0/0/0}
 - **SWITCH(config-Line)#**
 - To configure line passwords {Console, aux, vty}
 - **SWITCH(config-router)#**
 - To configure routing protocols {RIP, EIGRP, OSPF....}
- **Rx-boot Configuration Mode i.e. ROMMON>**
 - Trouble-shooting
 - Password Recovery
- **Setup Mode/ Initial Configuration Mode i.e. {yes/no}**
 - If there is no startup-config in the NVRAM
 - New SWITCH



IOS Modes - Commands

- **SWITCH>**
- **SWITCH > enable**
- **SWITCH # Configure Terminal**
- **SWITCH (config)# Interface fastEthernet 0/0**
- **SWITCH (config-if)# exit**
- **SWITCH (config)# exit**
- **SWITCH # exit**
- **Exit from SWITCH & press enter**
- **SWITCH>**

Cisco IOS- Basic Configuration

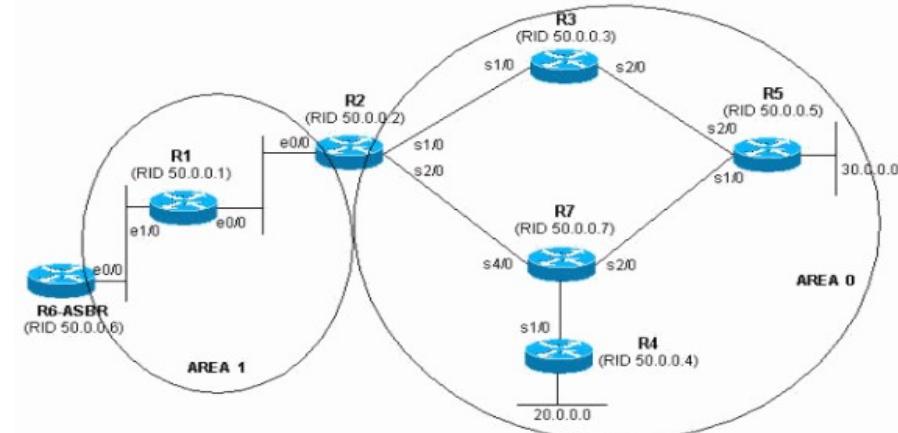
- **Show commands**
 1. **SWITCH# show running-config**
 - To check the RAM contents
 2. **SWITCH # show startup-config**
 - To check the NVRAM contents
 3. **SWITCH# show flash:**
 - To check the flash memory
 4. **SWITCH# show version**
 - To check IOS version {Registry setting i.e. CRV code}
 5. **SWITCH# show interface**
 - To check all SWITCH interface configuration & status
 6. **SWITCH# show interface fa 0/1**
 - To check interface configuration & status
 7. **SWITCH# show ip interface brief**
 - To check all interface status {L1 & L2} & ip address
 8. **SWITCH# show line**
 - To verify all line & usable lines

Switching Technologies

IOS Basics

Lab 1 - Basics

Lesson 11

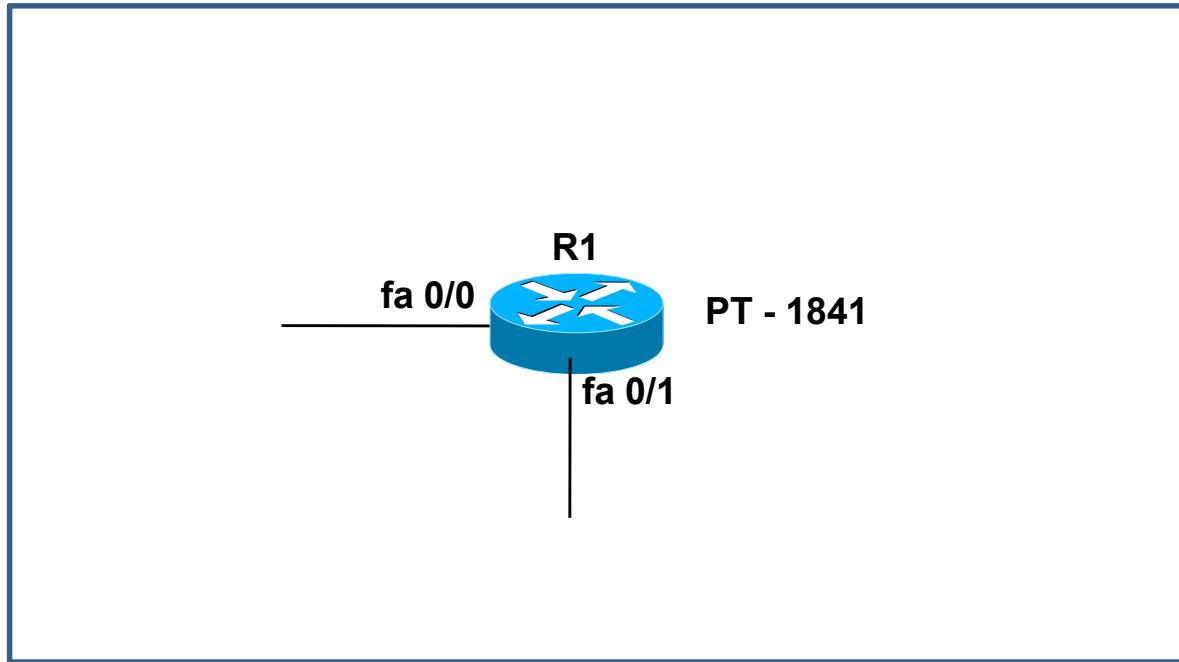


Lab 1 – IOS Basics - Concepts

1. Modes
2. Host Name
3. Passwords: i.e. Password Policy: All = cisco, On demand = class
 - a) Line:
 - I. Console {0}
 - II. Aux {0}
 - III. VTY {0-15}
 - b) Enable:
 - I. Enable – Normal
 - II. Enable – Secret
 - c) All passwords encrypted in Running-config
4. Message
5. Save i.e. RAM to NVRAM
6. How to delete a command? i.e. Console Password
7. Show Commands
8. Help Commands i.e. ?, Tab key, up/Down arrow keys & More..... – Enter/space bar
9. Show cdp neighbours i.e. CDP = Cisco Discovery Protocol

*** Password Policy for Labs:
All Passwords = cisco
On Demand = class

Lab 1 – Basics - Topology



- **Host Name**
 - Router(config)# hostname R1
 - R1 (conf ig)#

Lab 1 – Basics - Commands

- Router Password Configuration
 - Line Console Password:
 - Router> enable
 - Router# configure terminal
 - Router(config)# line console 0
 - Router(config-line)# password cisco
 - Router(config-line)#login
 - Router(config-line)#exit
 - Router(config)#exit
 - Router#exit
 - Press Enter.....Password:ciscoRouter>
 - Router Password Configuration
 - Line Aux Password:
 - Router> enable
 - Router# configure terminal
 - Router(config)# line aux 0
 - Router(config-line)# password cisco
 - Router(config-line)#login
 - Router(config-line)#exit
 - Router(config)#exit
 - Router#



Lab 1 – Basics - Commands

- **Router Password Configuration**

- **Line VTY Password:**

- Router> en
 - Router# configure terminal
 - Router(config)# line vty 0 15 {i.e. 16 virtual terminals}
 - Router(config-line)# password cisco
 - Router(config-line)#login
 - Router(config-line)#exit
 - Router(config)#exit
 - Router#

- **Router Password Configuration**

- **Enable Password:**

- Router> enable
 - Router# configure terminal
 - Router(config)# enable password cisco
 - Router(config)#exit
 - Router#exit
 - Press enter
 - Passsword:
 - Router> enable
 - Password:



Lab 1 – Basics - Commands

- **Router Password Configuration**
 - Enable secret Password:
 - Router> enable
 - Router# configure terminal
 - Router(config)# enable secret class
 - Router(config)#exit
 - Router#exit
 - Press enter
 - Passsword:
 - Router> enable
 - Password:
 - To Encrypt all password in the running - config
 - ***Router(config)# service password-encryption
- **Message**
 - Router(config)# banner motd \$Have a nice day\$
- **Save i.e. RAM to NVRAM**
 - Router# copy running-config startup-config
- **Help**
 - ? = options, Tab key = Command auto-completion, Up/Down arrow keys = History Commands, More = Enter {Line by Line} & Space bar {Page by Page}
- **Delete a command**
 - Copy the command for running-config
 - Go to the exact mode, where we config & type “no” and paste the full command. That’s all.

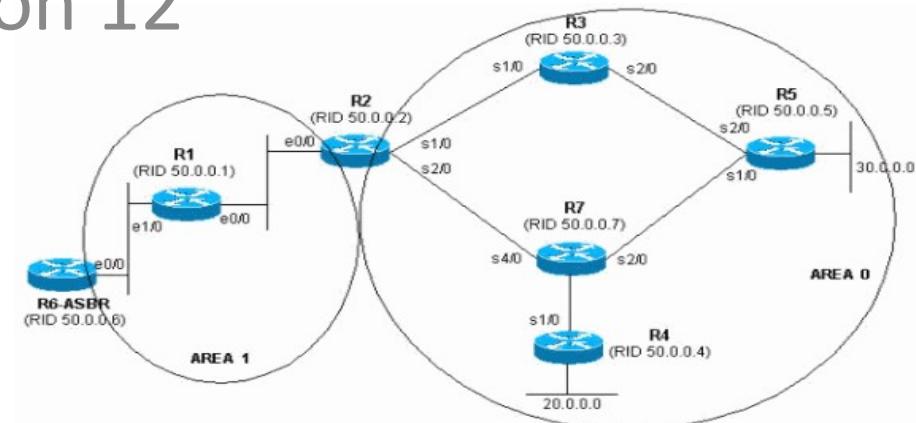


Switching Technologies

IOS Basics

Lab 2 – Telnet

Lesson 12



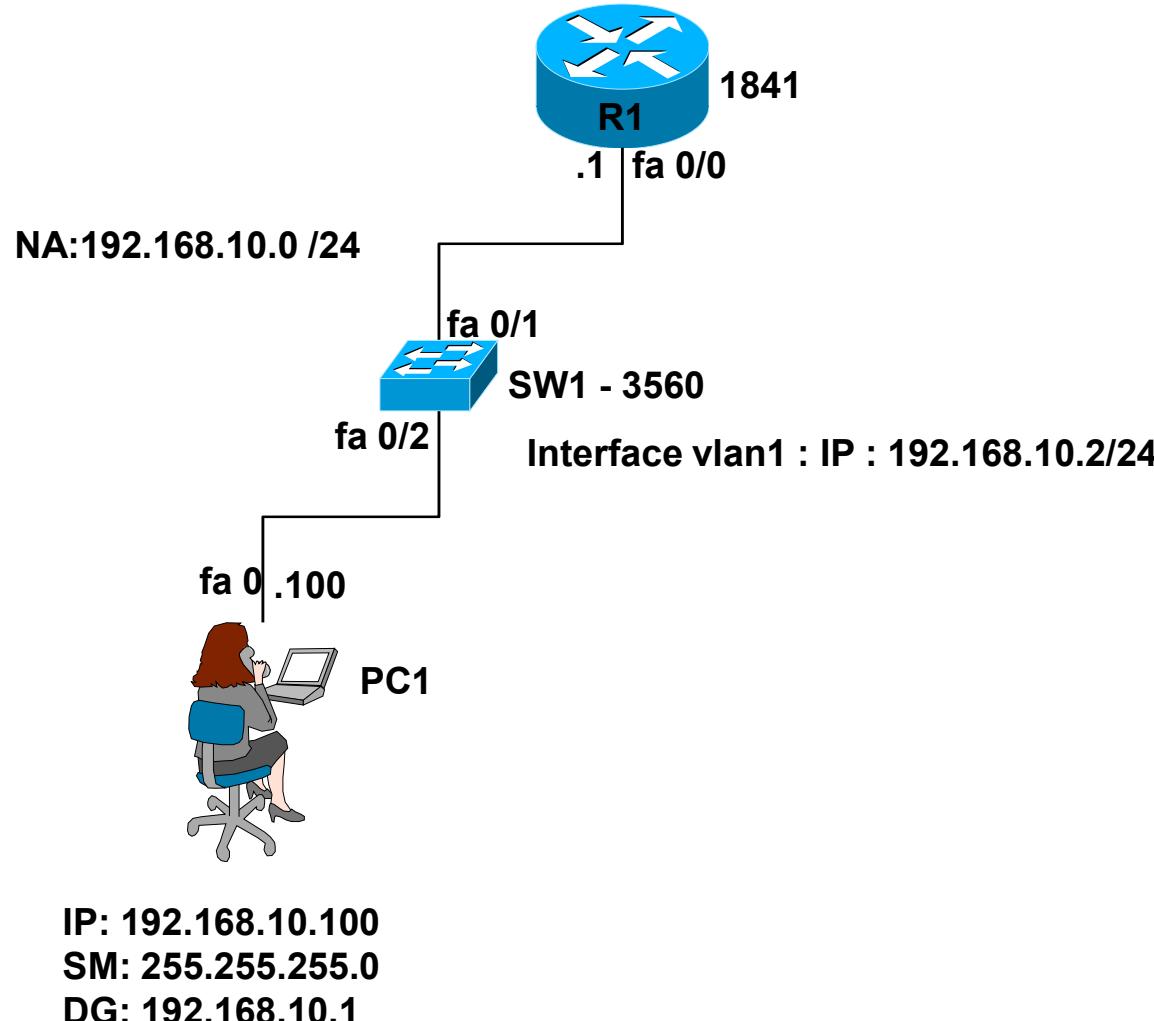
Lab 2 – Telnet - Concepts

0. Topology
1. Host Name {PT & Host}
2. IP Address
 1. PC1
 2. R1:Fa 0/0
3. R1 :
 1. Console password
 2. VTY password
 3. Enable password {normal}
4. PC1:
 1. Ping 192.168.10.100
 2. Ping 192.168.10.1
5. PC1: Telnet:
 1. CMD>Telnet 192.168.10.1
 - Password:
 - R1>



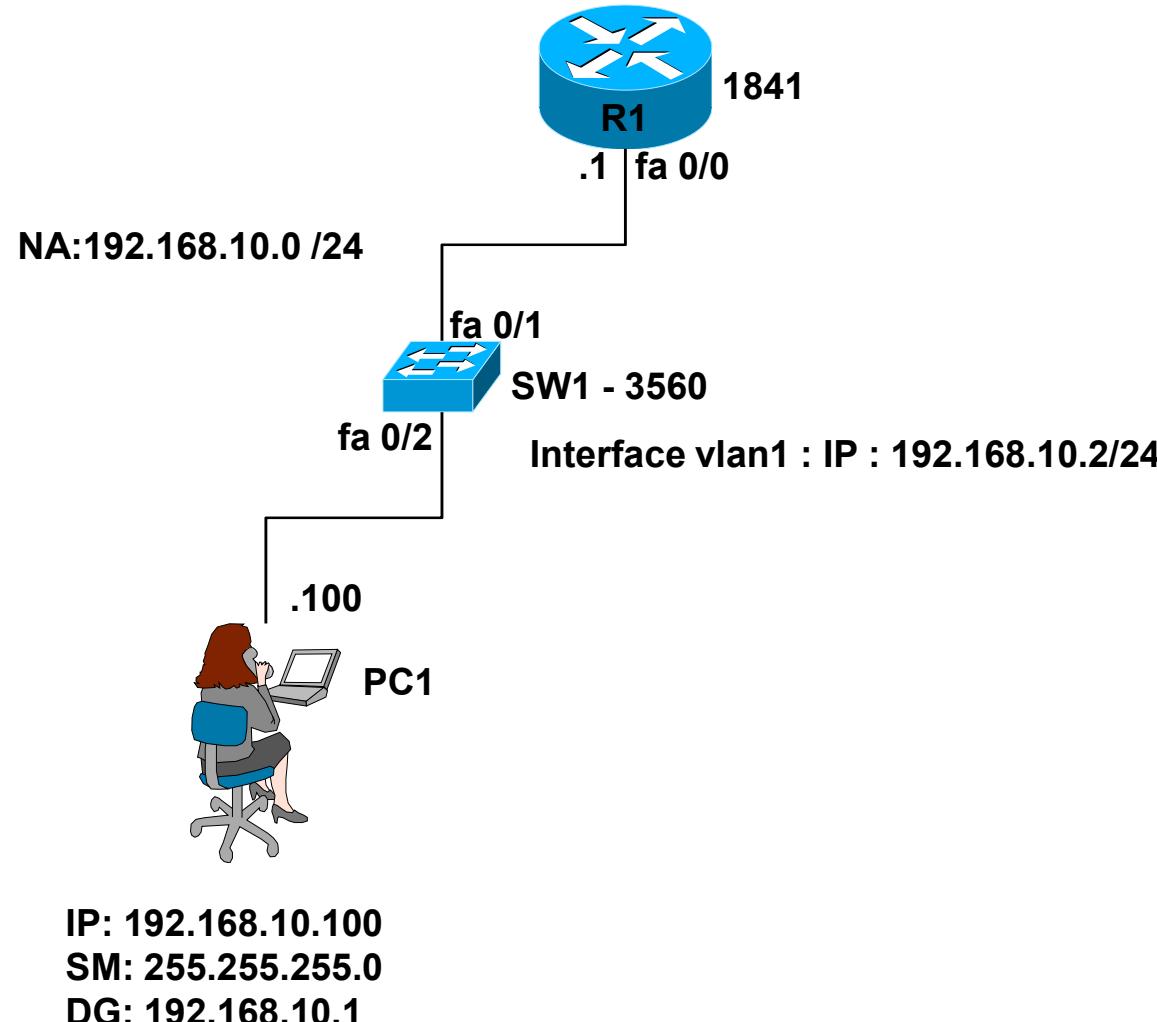
Lab 2, 3 & 4

Telnet/SSH/SW-MGT IP - Topology



Lab 2,3 & 4

Telnet/SSH/SW-MGT IP - Topology



Lab 2 – Telnet - Commands

- Router interface Configuration
 - Fast Ethernet 0/0
 - R1> enable
 - R1# configure terminal
 - R1(config)# interface fa 0/0
 - R1(config-if)# ip address 192.168.10.1 255.255.255.0
 - R1(config-if)# no shutdown
 - R1(config-if)# exit
- PC's Config:
 - Telnet Config
 - CMD> ipconfig
 - CMD> ping 192.168.10.1
 - CMD> telnet 192.168.10.1
 - Password: cisco
 - R1# enable
 - Password: cisco

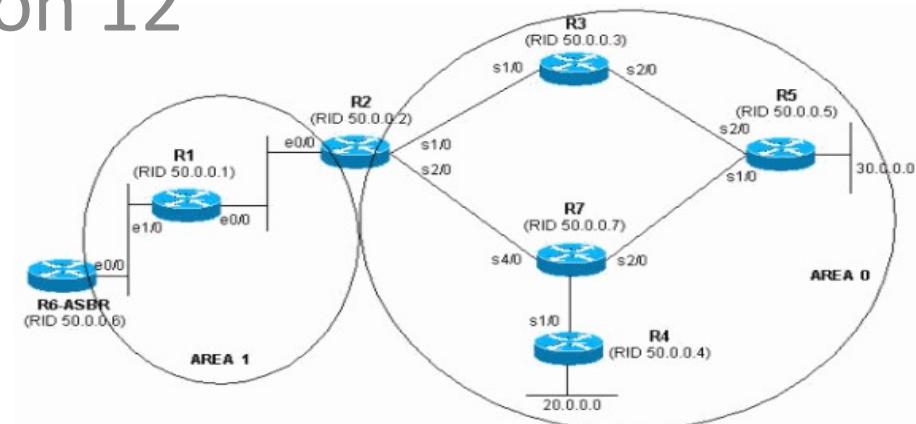


Switching Technologies

IOS Basics

Lab 3 – SSH {vty}

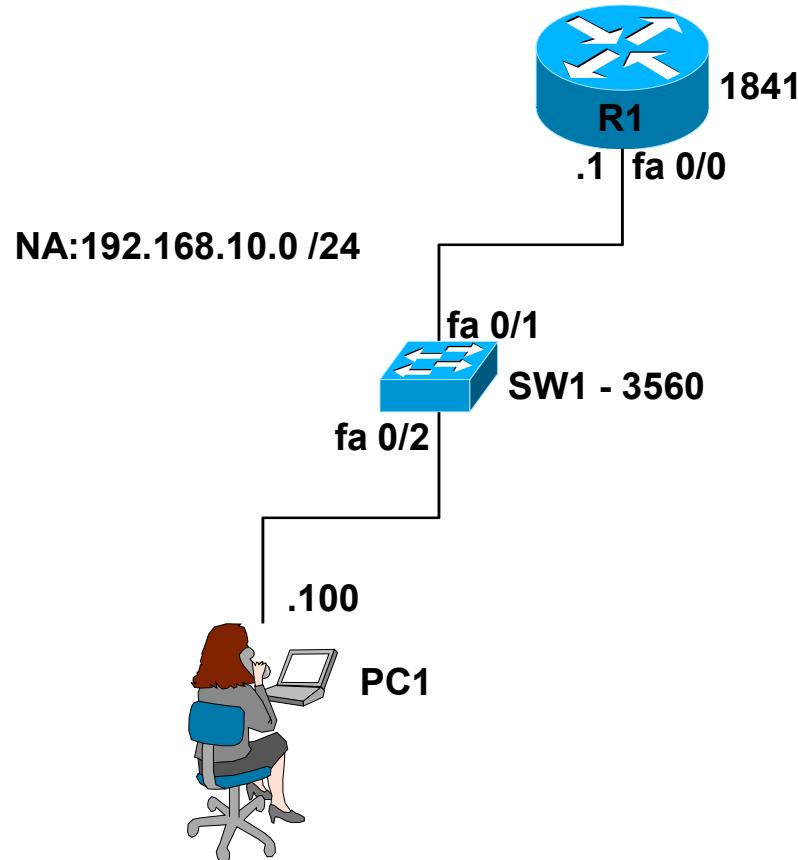
Lesson 12



Lab 3 – SSH - Concepts

0. Topology
1. Host Name {PT & Host}
2. IP Address
 1. PC1
 2. R1:Fa 0/0
3. R1 :
 1. Console password
 2. VTY password i.e. Login Local – UN: admin & PSSWD: cisco
 3. Enable password {normal}
4. R1: SSH:
 1. Configure ip domain-name
 2. Generate keys for 1024 bits
 3. Change ssh version 2
5. PC1:
 1. Ping 192.168.10.100
 2. Ping 192.168.10.1
6. PC1: ssh:
 1. CMD>ssh -l admin 192.168.10.1
 - Password: [vty password]
 - R1>

Lab 3 - SSH Topology



IP: 192.168.10.100
SM: 255.255.255.0
DG: 192.168.10.1



Lab 2 - SSH - Commands

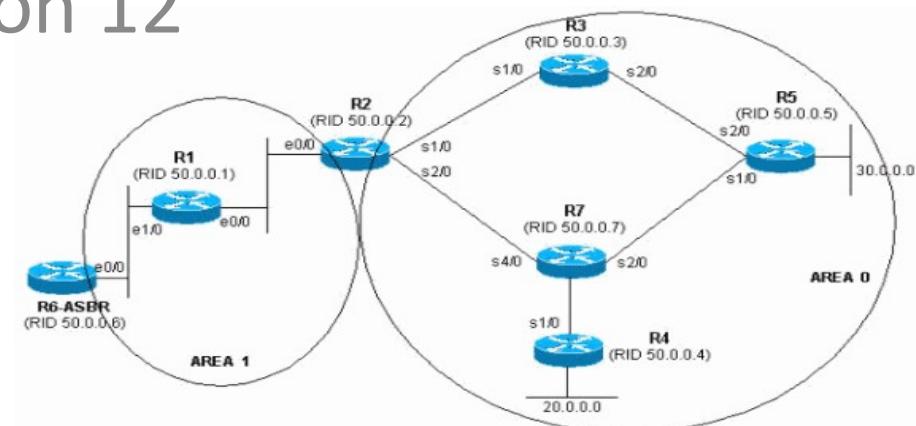
- **IP Domain**
 - R1(config)# ip domain-name cisco.com
- **Generate keys (modus=1024 bits)**
 - **SSH Config**
 - R1(config)# crypto key generate rsa
- **ssh version**
 - R1(config)# ip ssh version 2
- **PC's Config:**
 - **Telnet Config**
 - CMD> ipconfig
 - CMD> ping 192.168.10.1
 - CMD> ssh -l username 192.168.10.1

Switching Technologies

IOS Basics

Lab 4 –Switch_MGT IP

Lesson 12

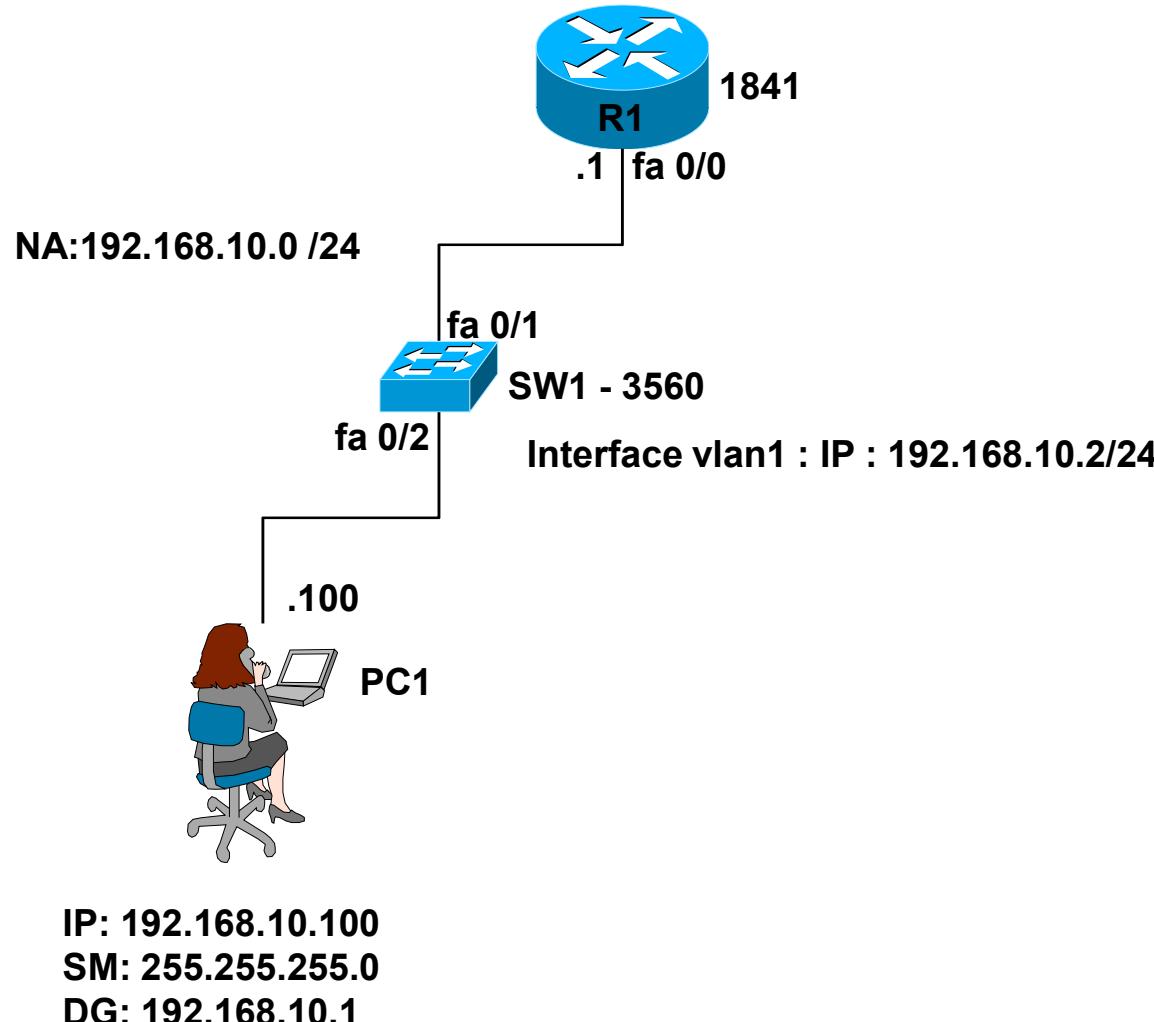


Lab 4 – MGT IP - Concepts

0. Topology
1. Host Name {PT & Host}
2. IP Address
 1. PC1
 2. SW1:VLAN 1 interface
3. SW1:
 1. Console password
 2. Vty password
 3. Enable password {normal}
4. PC1:
 1. Ping 192.168.10.100
 2. Ping 192.168.10.2
5. PC1: Telnet:
 1. CMD>telnet 192.168.10.2
 - Password: [vty password]
 - SW1>



Lab 4 - SW-MGT IP - Topology



Lab 4 –SW MGT IP- Commands

- **Interface VLAN 1 IP:**
 - **SW1(config)# interface VLAN1**
 - **SW1(config-if)# ip address 192.168.10.2 255.255.255.0**
 - **SW1(config-if)# no shut**
 - **SW1(config-if)# exit**
- **PC's Config:**
 - **Telnet Config**
 - **CMD> ipconfig**
 - **CMD> ping 192.168.10.2**
 - **CMD> telnet 192.168.10.2**

LAN Switching Technologies

VLAN {Lab 5}

Lesson 26



VLAN/Trunk/VTP Concepts

➤ VLAN

- Virtual Local Area Network
- Virtually dividing one physical switch to multiple switches {VLANS}
- Segmenting Broadcast domains

➤ Trunk

- Link between two VLAN switches
- Allows all VLAN traffic
- Do VLAN tagging or encapsulation with ISL or DOT1Q

➤ VTP

- VTP = VLAN Trunking port
- Centralized VLAN configuration
- Three modes i.e. Server, Transparent & Client

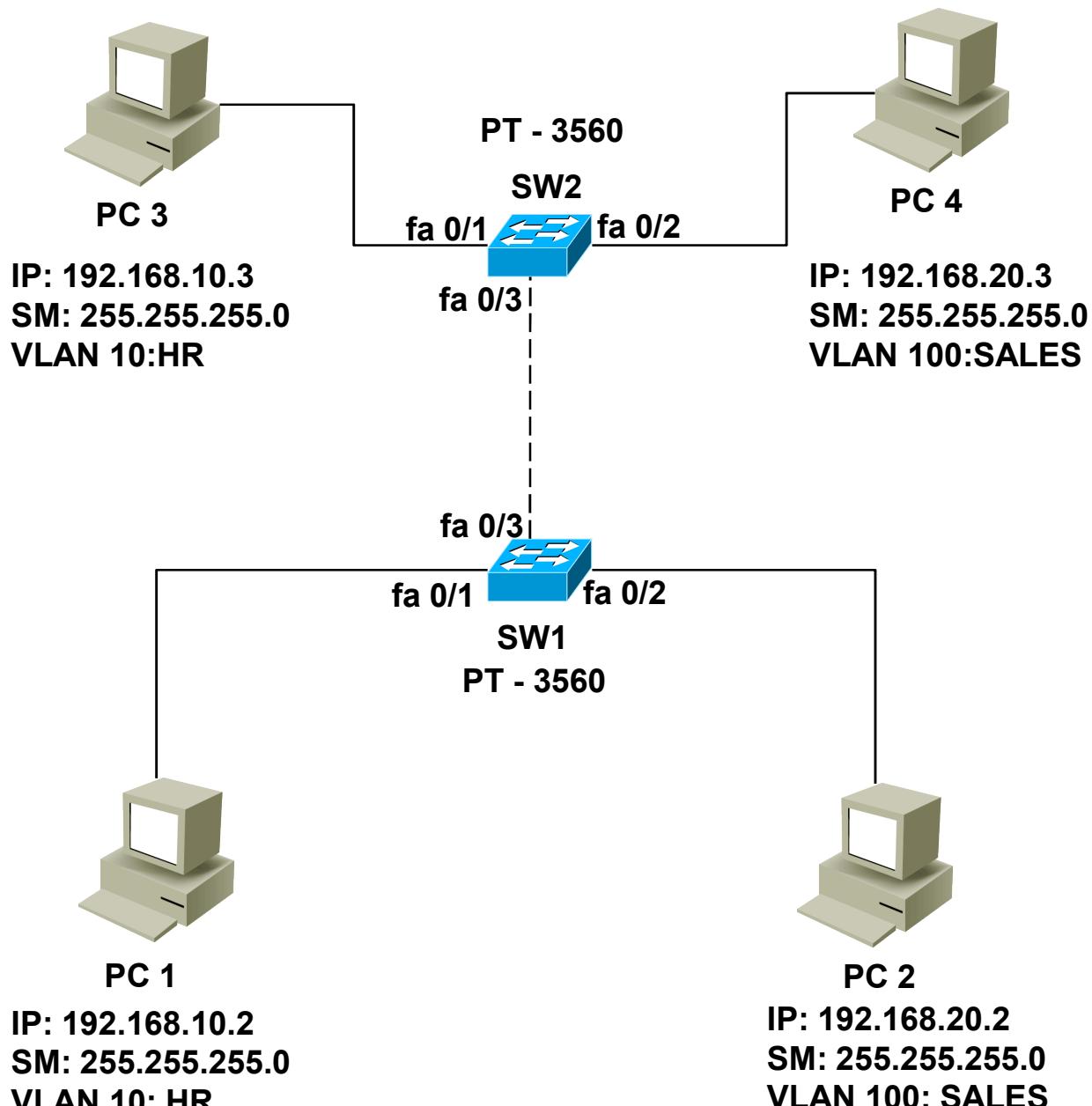
VTP Modes

- SERVER [Default]
 - Creates VLAN's
 - Saves VLAN's information
 - Send & Receive VTP updates
 - VLAN database will be updated based on VTP updates
- Transparent
 - Send & Receive VTP updates
 - No changes based on VTP updates
 - Create & Save VLAN information
- CLIENT
 - Send & Receive VTP updates
 - VLAN database will be updated based on VTP updates
 - Not create or save any VLAN information

VLAN - LAB Concepts

0. Topology
1. Host Names
2. Ip address
3. Configure VLANs
4. Assign ports to the VLANs
5. Verify the VLAN
 1. Ping PC1 to PC3
 2. Ping PC2 to PC4

VLAN - Topology



VLAN - Commands

- To config VLANS:
 - SW1# configure terminal
 - SW1(config)# vlan 10
 - SW1(config-vlan)# name HR
 - SW1(config-vlan)# exit
- To assign ports to VLAN:
 - SW1(config)#interface fastethernet 0/1
 - SW1(config-if)#switchport mode access
 - SW1(config-if)#switchport access vlan 10
 - SW1(config-if)#exit
- To verify VLANS:
 - SW1# show VLAN brief

LAN Switching Technologies

Trunk {Lab 6}

Lesson 27

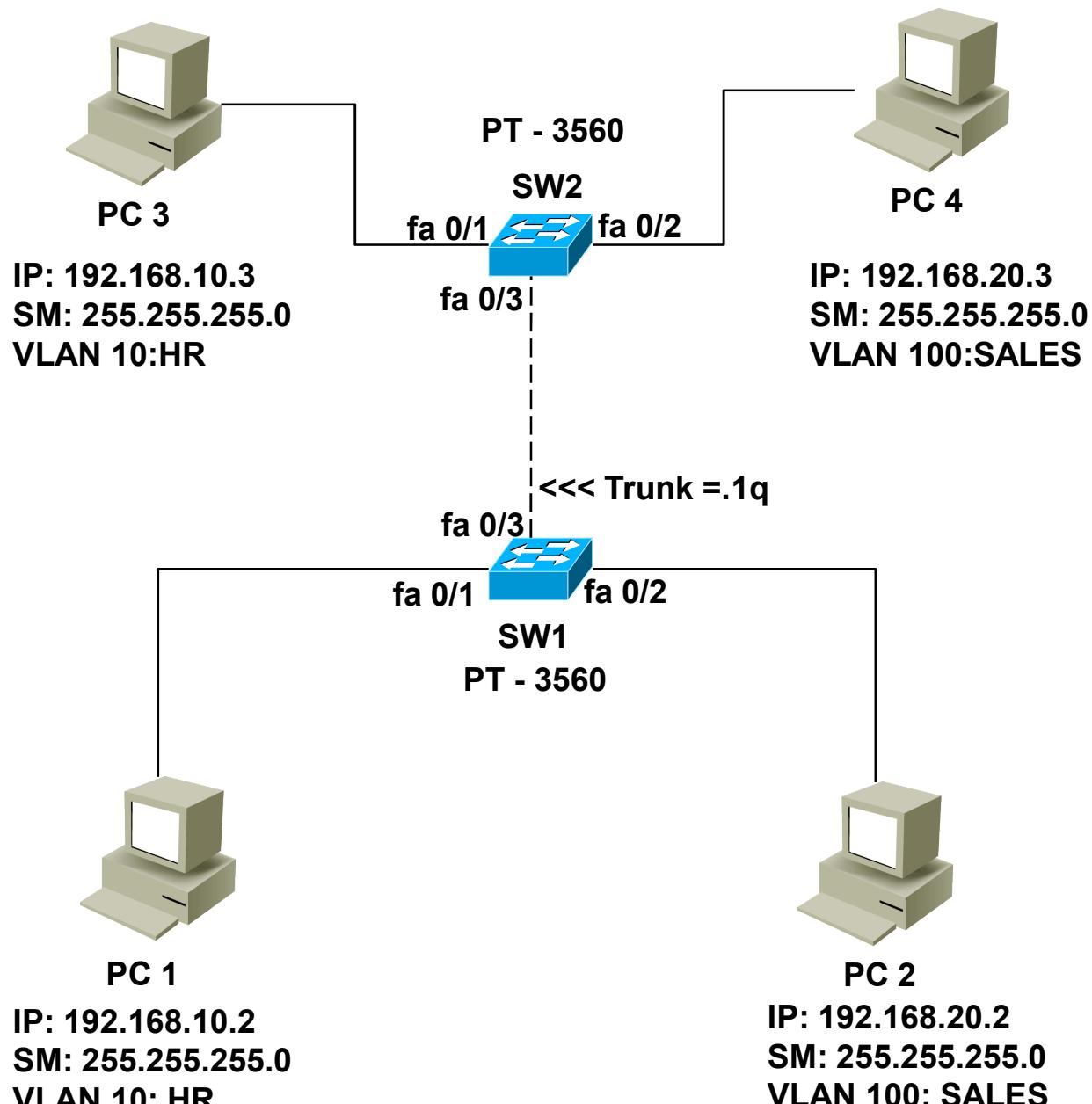


Trunk - LAB Concepts

0. Topology
1. Host Names
2. Ip address
3. Configure Trunk
 1. In Interface config mode
 2. Encapsulation with dot1q
 3. Set port mode as Trunk
4. Verify the Trunk



Trunk - Topology



TRUNK - Commands

- To assign trunk ports:
 - SW1(config)#interface fastethernet 0/3
 - SW1(config-if)#switchport trunk encapsulation dot1q
 - SW1(config-if)#switchport mode trunk
 - SW1(config-if)#exit
- To verify trunks:
 - SW1# show VLAN brief
 - SW1# show running-config
 - SW1#show interface trunk

LAN Switching Technologies

VTP {Lab 7}

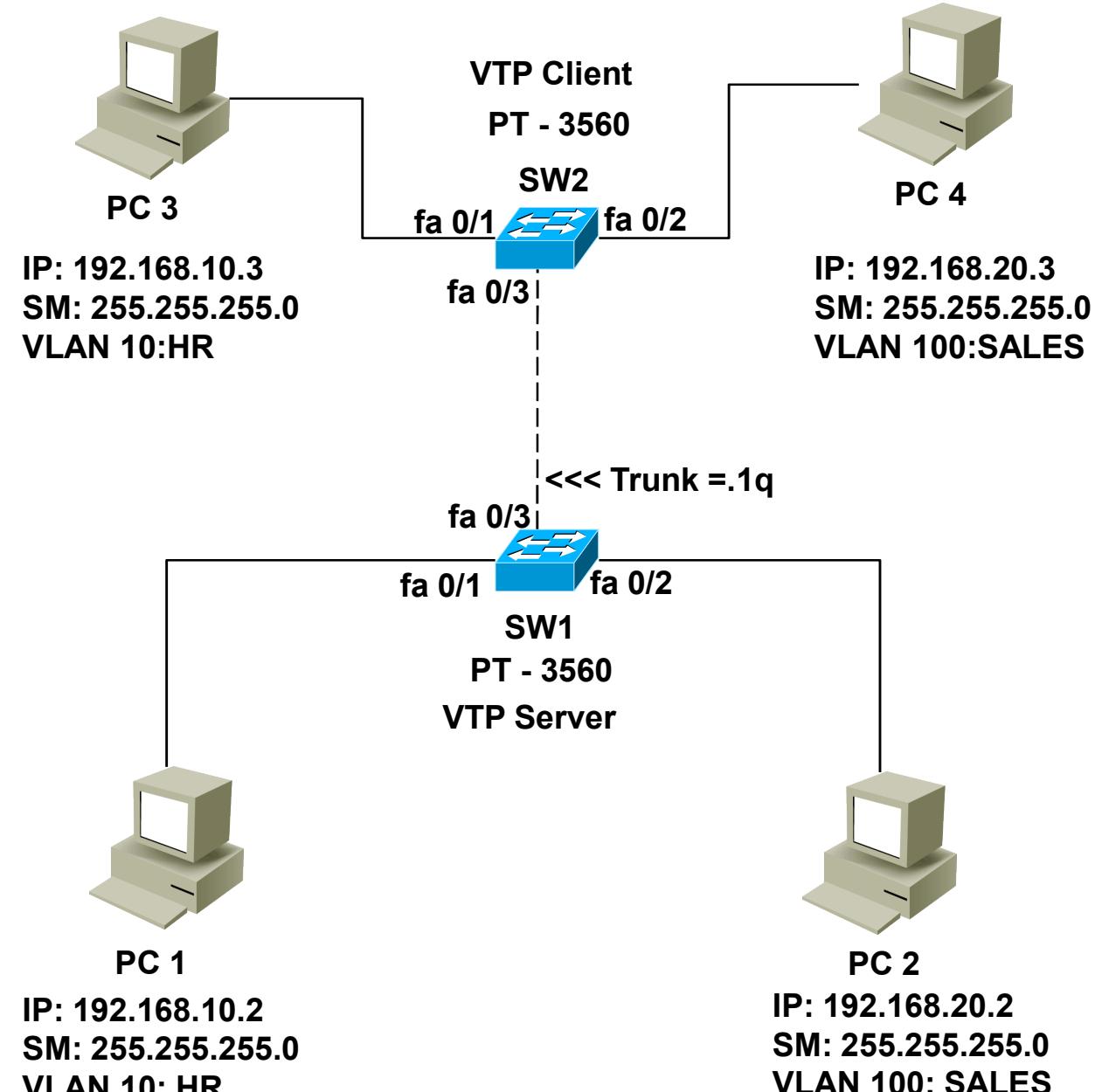
Lesson 28



VTP - LAB Concepts

0. Topology
1. Host Names
2. Ip address
3. Configure VTP
 1. In Global config mode
 2. VTP Domain Name
 3. VTP Mode Server/Client/Transparent
4. Verify VTP

VLAN/TRUNK/VTP - Topology



VTP - Commands

- To configure VTP:
 - SW1(config)#vtp domain cisco
 - SW1(config)#vtp mode server
- To verify trunks:
 - SW1# show vtp status

LAN Switching Technologies

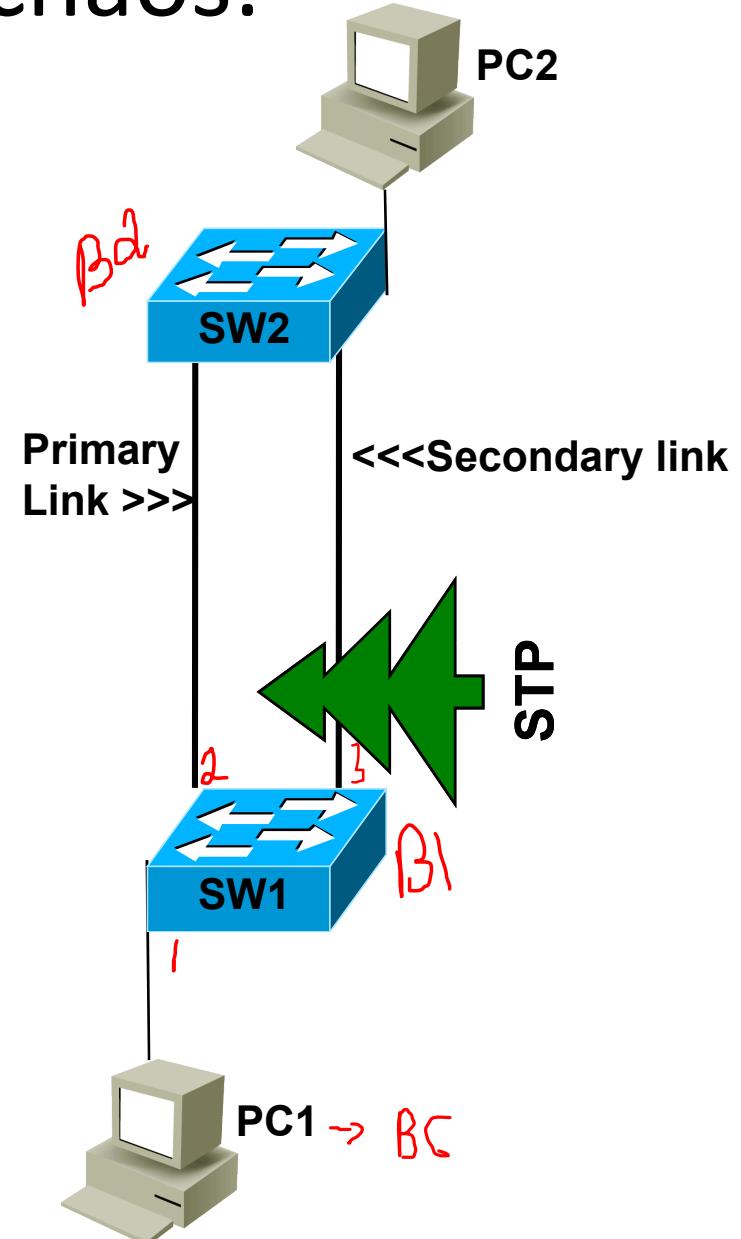
STP, PVST+, RSTP

Lesson 29



Redundancy chaos:

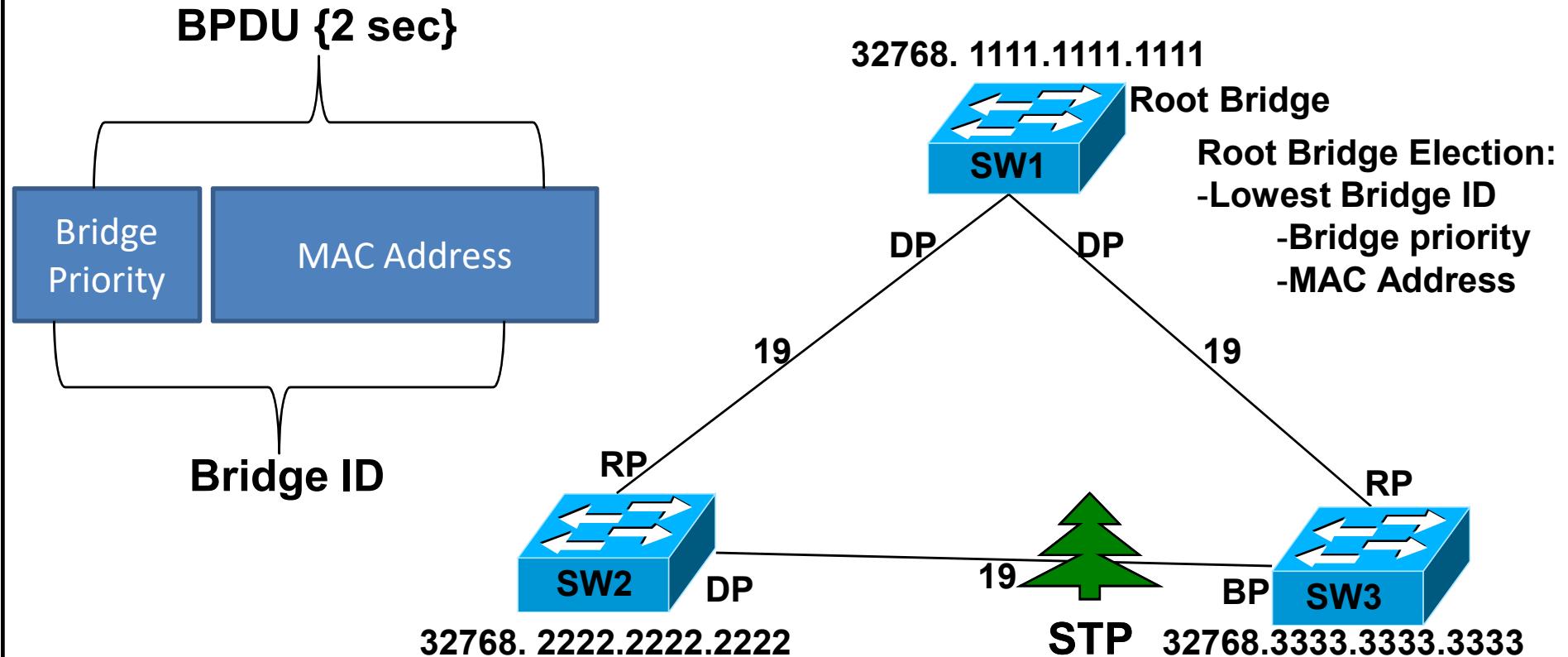
- Switches Forward Broadcast packets out in all ports by design
- Redundant connections are necessary in business networks
- The place of Spanning Tree:
 - Drop Trees on the redundant links



Key facts about STP

- Original STP(802.1D/ieee) was created to prevent loops
- Switches send “probes” into the network called Bridge Protocol Data units (BPDU) to discover loops
- The BPDU probes also Help to elect the core switch of the network, called the root bridge
- The simplistic view of STP:
 1. Election of Root Bridge {RB}
 2. All other switches find best way to reach RB
 3. Block{Drop trees} all redundant links

Understanding BPDU & Elections



STP Port Roles & Responsibilities:

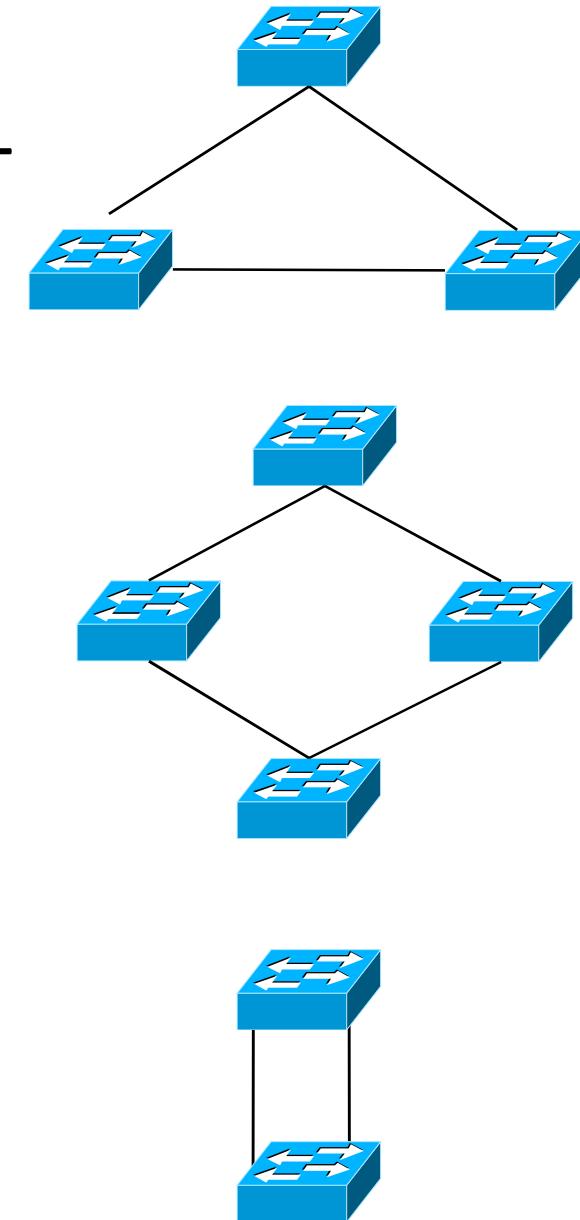
- Root Port: used to reach the root bridge
- Designated port: Forwarding port, one per link
- Blocking/Non-Designated port: Where the tree falls



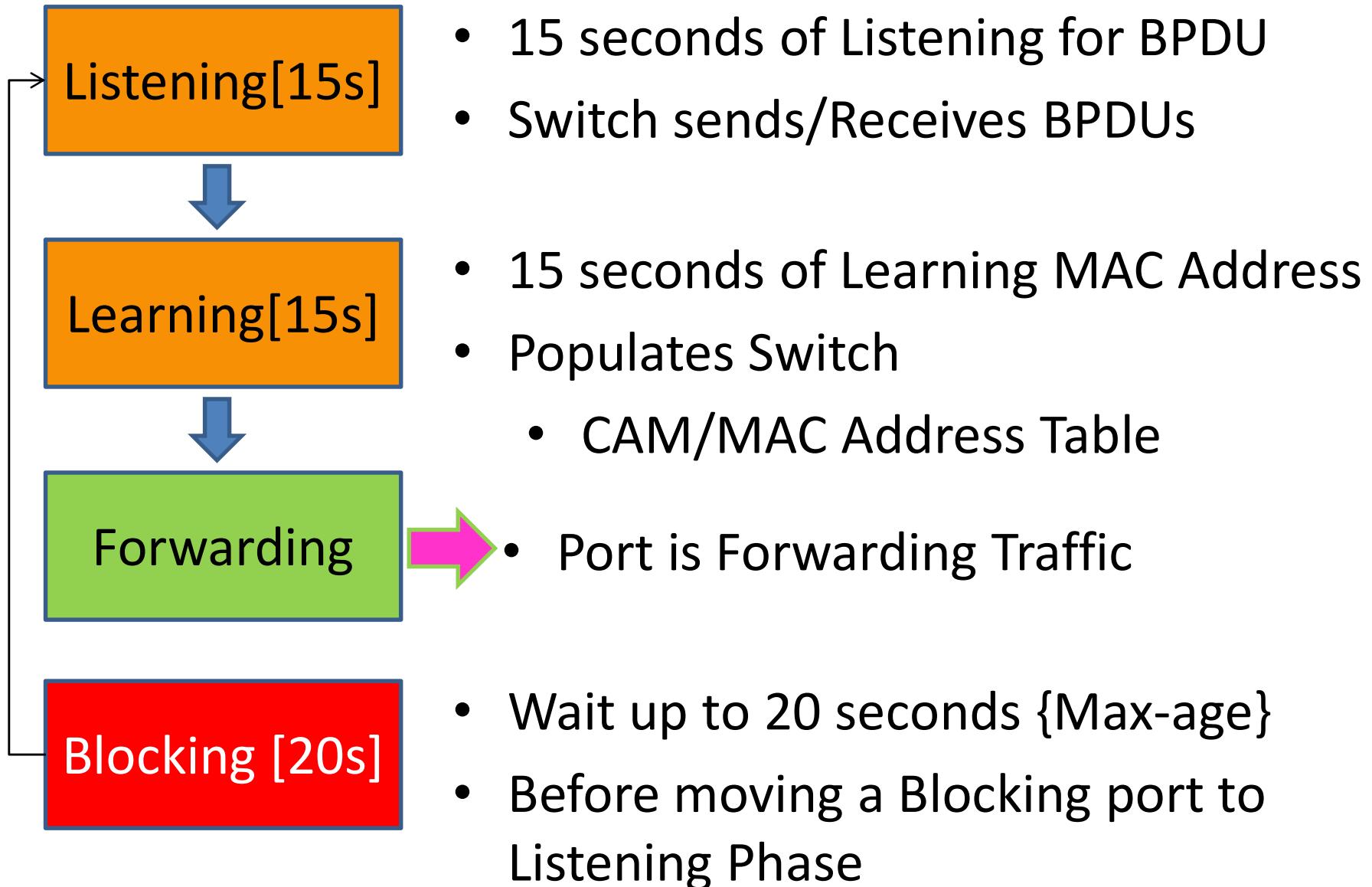
How STP finds the Best Path

- Elect the Root Bridge
- Find the Best path to the ROOT
 - Lowest link cost
 - Lowest Bridge ID
 - Lowest Port Number
- Block whatever is left over
 - COST Table:

Link Bandwidth	COST
10 Mbps	100
100 Mbps [Fa]	19
1 Gbps [Gig]	4
10 Gbps [10G]	2



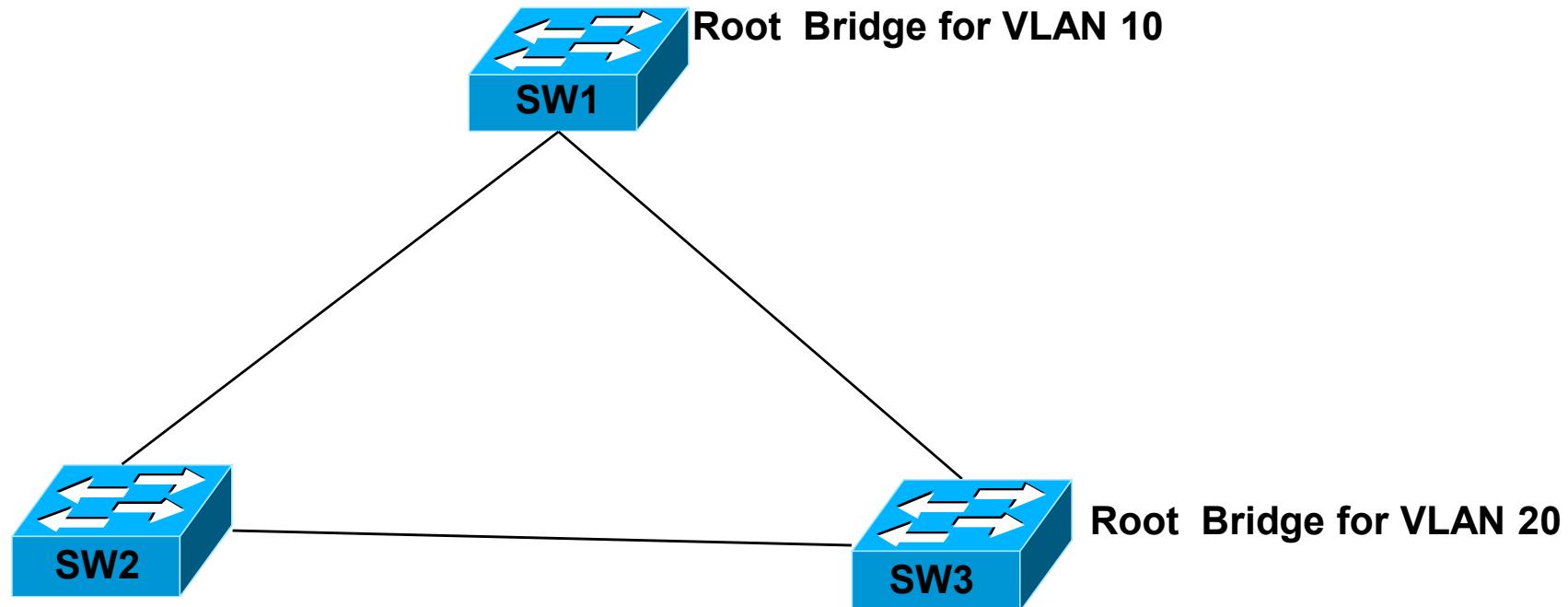
STP Port State Transitioning Process



Problems & Solutions

- Problem with PC's:
 - 30 seconds
 - Solution: Port fast
 - Fa0/1:
 - Command: Switch(config-if)#spanning-tree port fast
 - Disable STP & directly goes to Forwarding port – **Use with Caution**
- Problems with Uplink ports:
 - $20+15+15=50$ seconds
 - Solution : Rapid pvst+

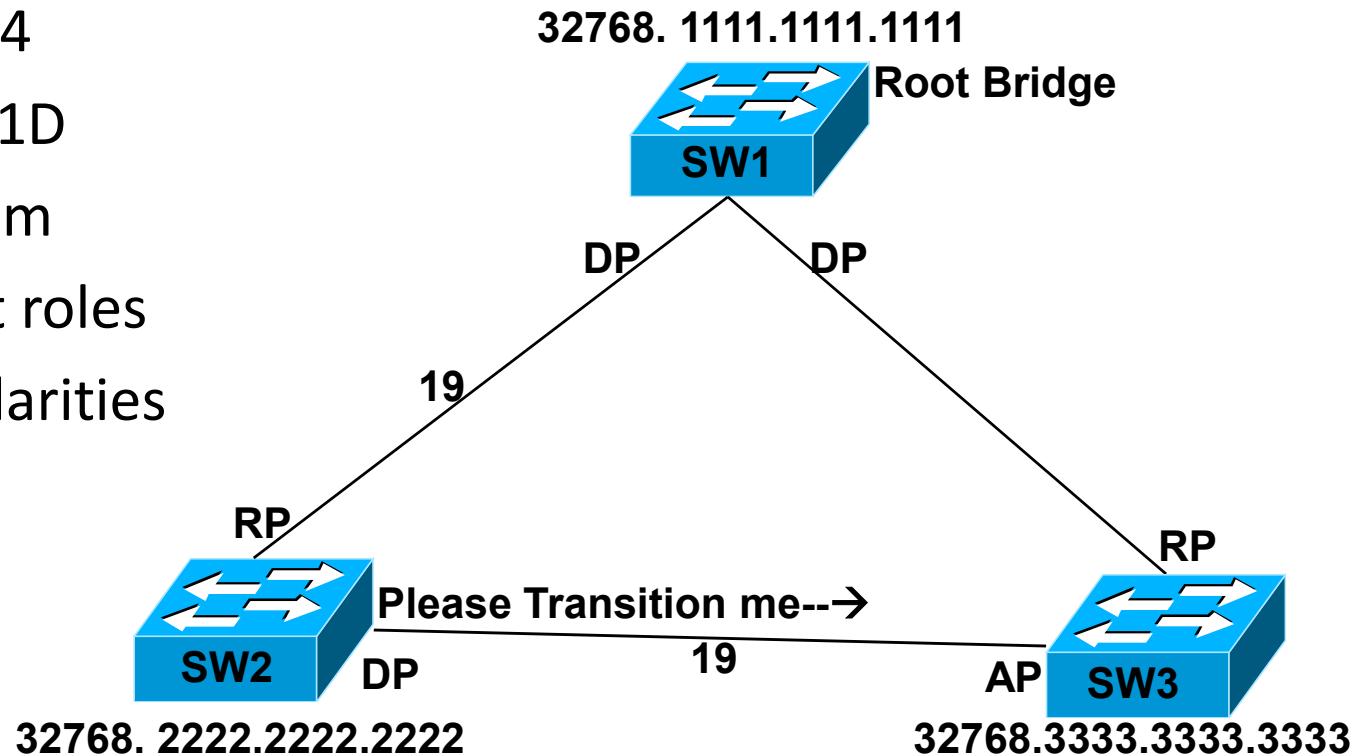
Initial STP Enhancement: PVSTP+



- Per VLAN Spanning-tree protocol
- Runs an instance of STP per VLAN
- Allows different Root Bridges per VLAN

How RSTP Improves Performance:

- Rapid STP: 2004
- 802.1W → 802.1D
- Proactive system
- Redefined port roles
- Many STP similarities



RSTP Port Roles:

- Root Port: used to reach the root bridge
- Designated port: Forwarding port, one per link
- Alternate port: Discarding port, Backup path to root



LAN Switching Technologies

Port Fast

Lab 8

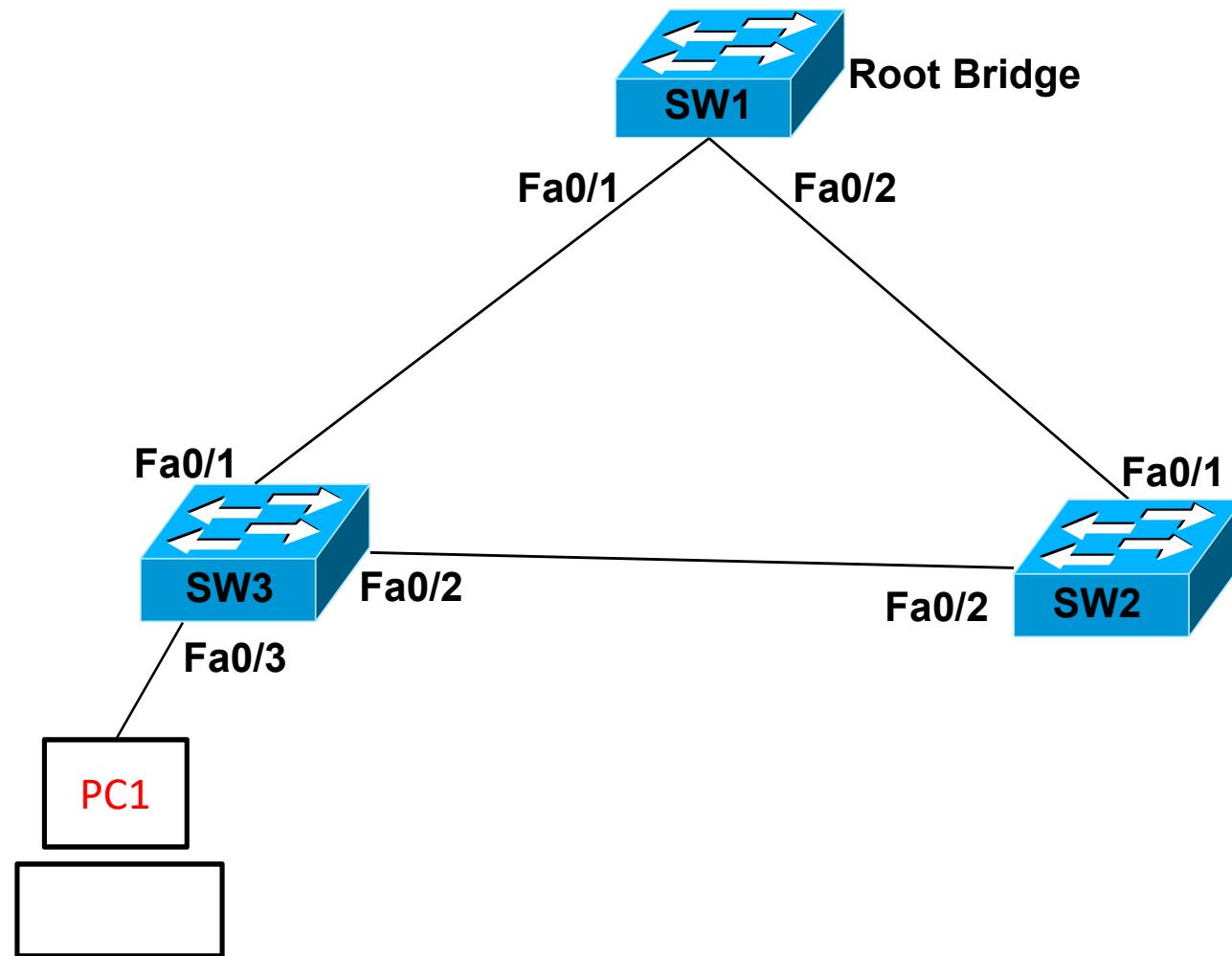
Lesson 29



Port fast - Concepts

0. Topology
1. Host Names
2. Port fast
 1. Connect a PC
 2. Configure portfast in that interface
 3. Re-connect the PC & verify STP transition state

Port fast/Root Bridge/RSTP - Topology



Port fast - Commands

- To verify:
 - SW1# show spanning-tree
- To configure port fast:
Fa0/3:
 - SW1(config-if)#spanning-tree port fast

LAN Switching Technologies

BPDU guard

Lesson 29

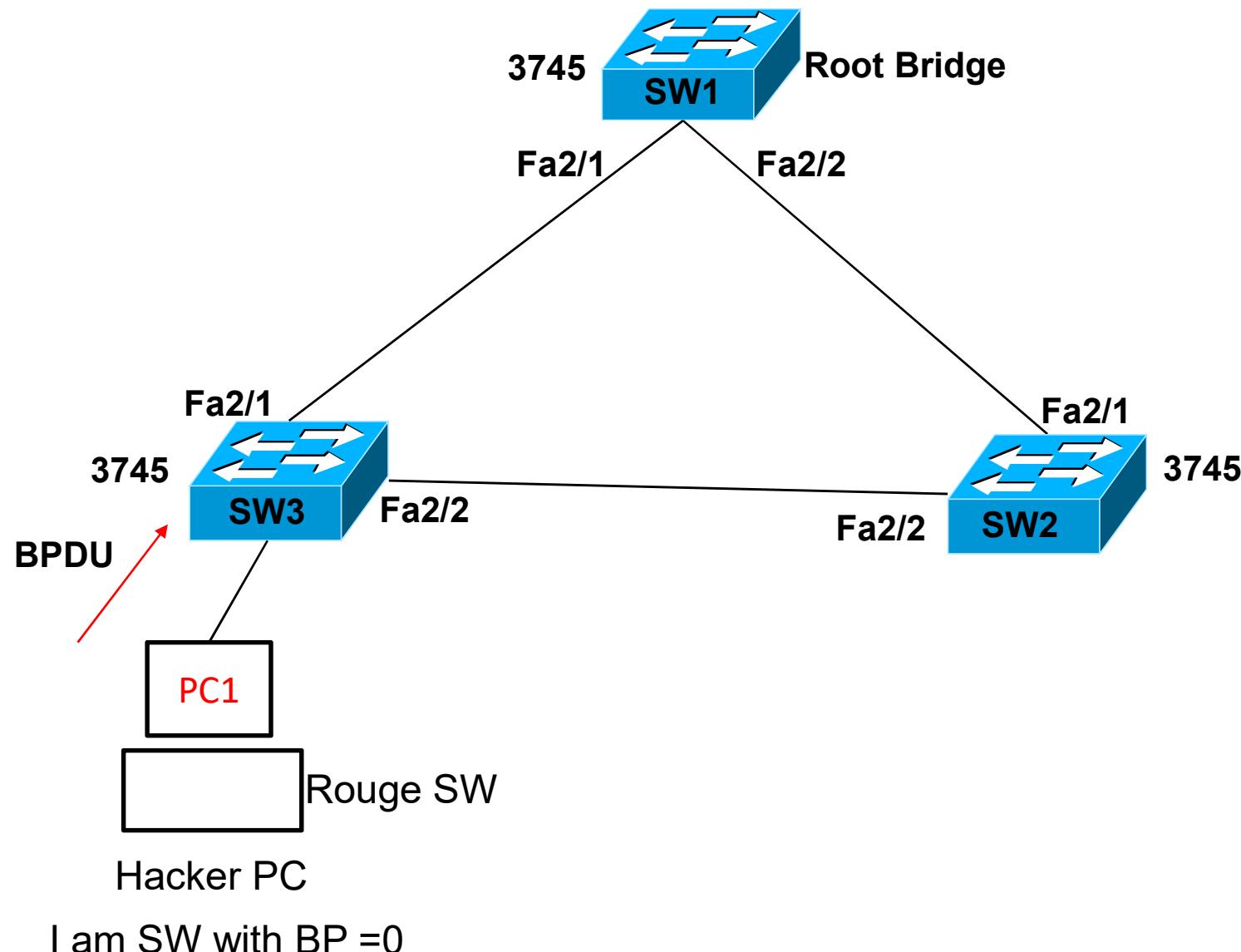


BPDU guard - Concepts

0. Topology
1. Host Names
2. Configure BPDU guard



BPDU guard - Topology



BPDU guard - Commands

- To verify:
 - SW1# show spanning-tree summary

- To configure bpduguard:

SW1:

- SW1(config)#spanning-tree port fast bpduguard

LAN Switching Technologies

STP – Root bridge

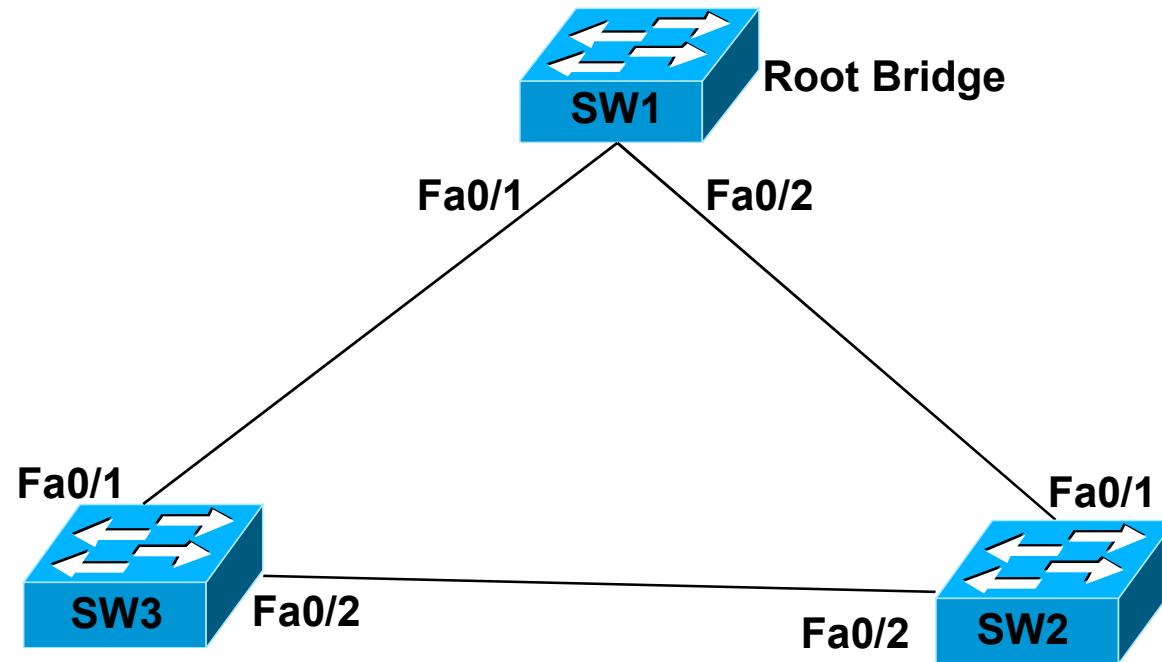
Lesson 29



Root bridge - Concepts

0. Topology
1. Host Names
2. Configure Root Bridge
3. Verify

Root bridge - Topology



Root bridge - Commands

- To verify:
 - SW1# show spanning-tree
- To change the Root bridge:
 - SW1(config)# spanning-tree VLAN 1 priority 4096

LAN Switching Technologies

STP – PVSTP+

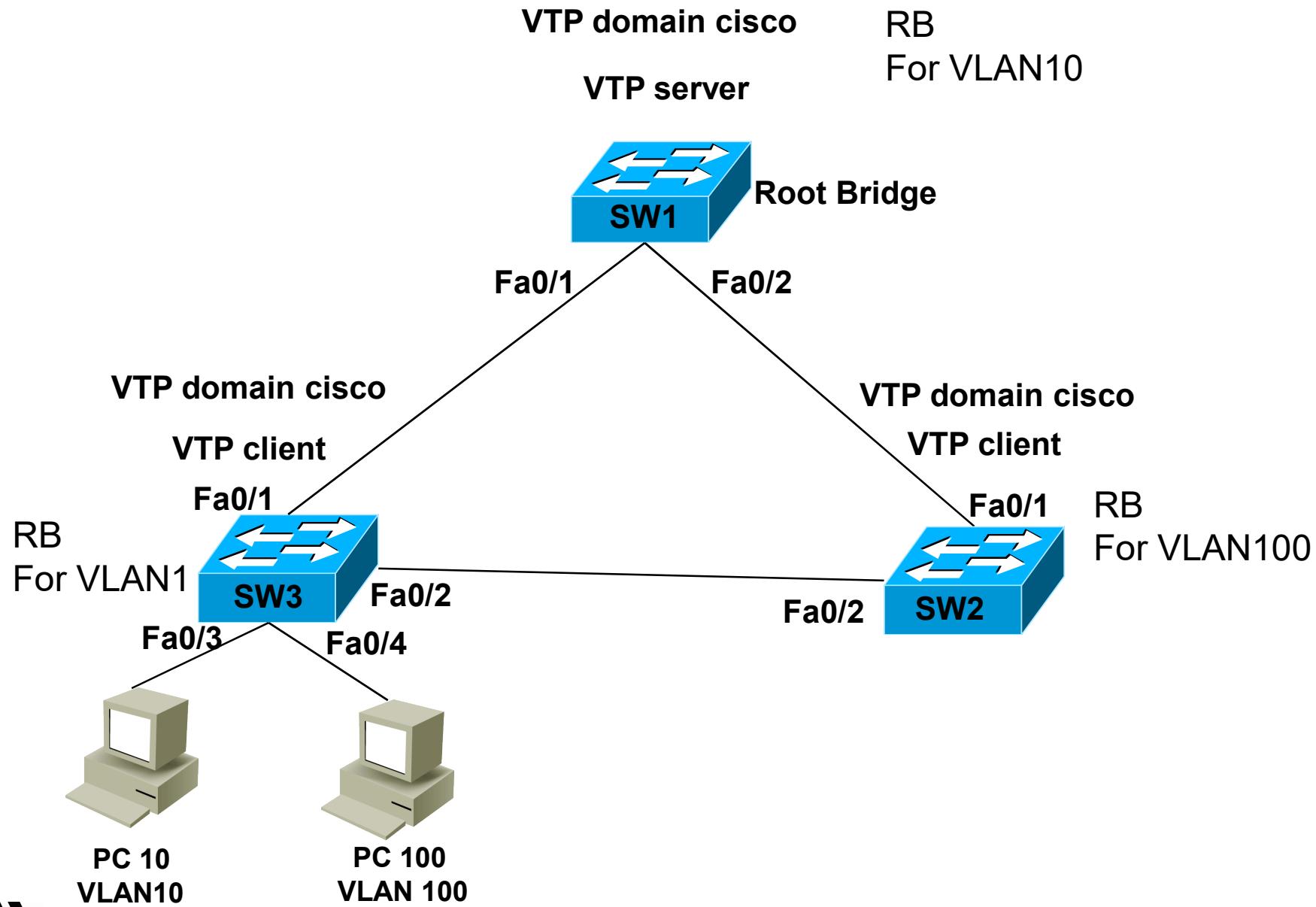
Lesson 29



PVSTP+ - Concepts

0. Topology
1. Host Names
2. Configure Trunk
3. Configure VTP
4. Create two VLANs i.e. 10 & 100
5. Assign interface to VLANs
6. Configure PVSTP+
7. Configure SW1 – RB for VLAN 10
8. Configure SW2 – RB for VLAN100
9. Verify

PVSTP+ - LAB 11 - Topology



STP/PVST+/RSTP LAB - Commands

- To verify:
 - SW1# show spanning-tree
- To change the Root bridge:
 - SW1(config)# spanning-tree VLAN 1 priority 4096
 - SW3(config)# spanning-tree VLAN 10 priority 4096
- To change from STP/ieee to PVST+
 - SW1(config)# spanning-tree mode pvstp

LAN Switching Technologies

STP – RSTP

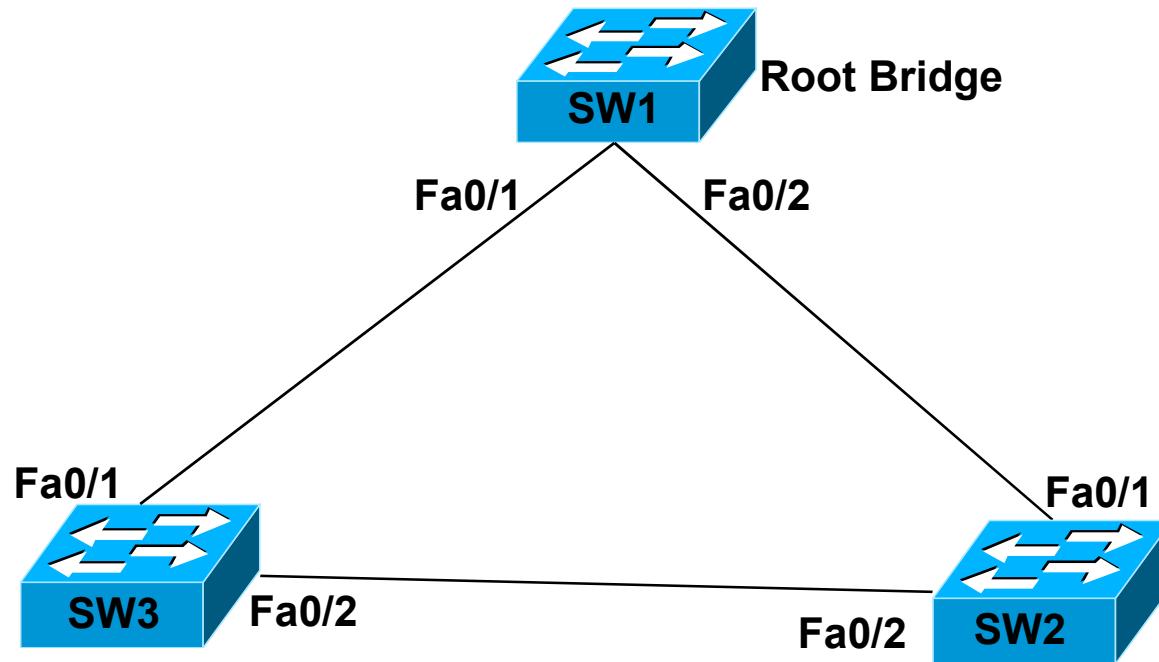
Lesson 29



RSTP - Concepts

0. Topology
1. Host Names
2. Configure RSTP
3. Verify

RSTP - Topology



RSTP - Commands

- To verify:
 - SW1# show spanning-tree
- To change from STP/ieee to RSTP:
 - SW1(config)# spanning-tree mode rapid-pvst

LAN Switching Technologies

CDP

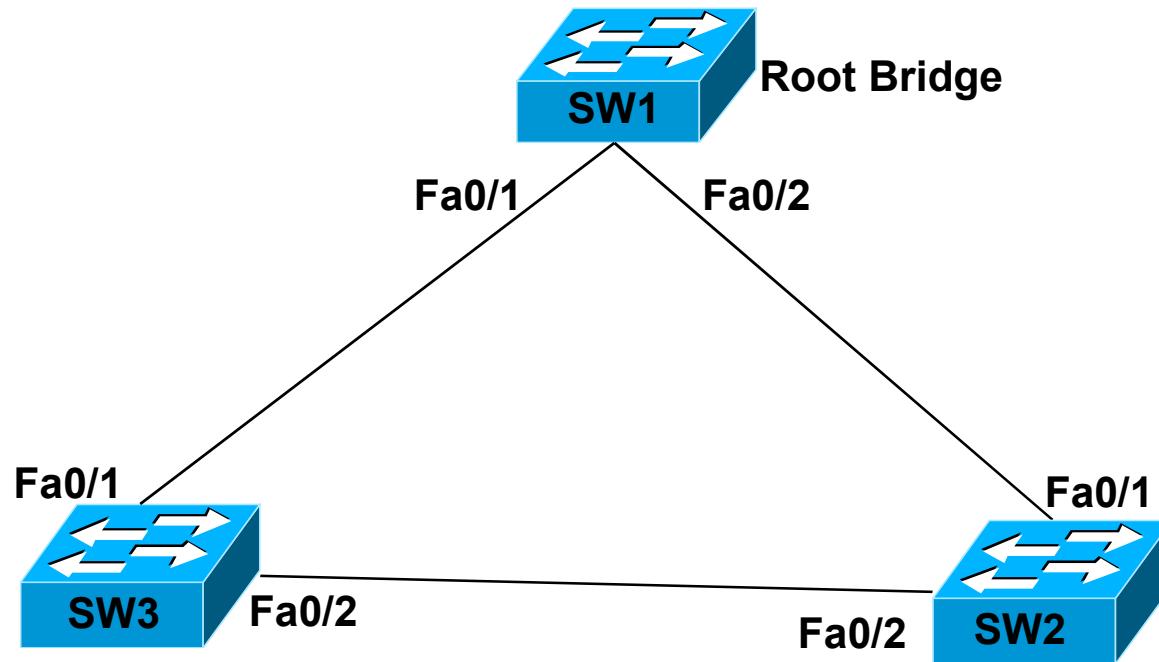
Lesson 29



RSTP - Concepts

0. Topology
1. Host Names
2. Configure CDP
3. Verify

RSTP - Topology



RSTP - Commands

- To verify:
 - SW1# show cdp neighbors
- To change from CDP:
 - SW1(config)# no CDP run/enable

LAN Switching Technologies

LLDP

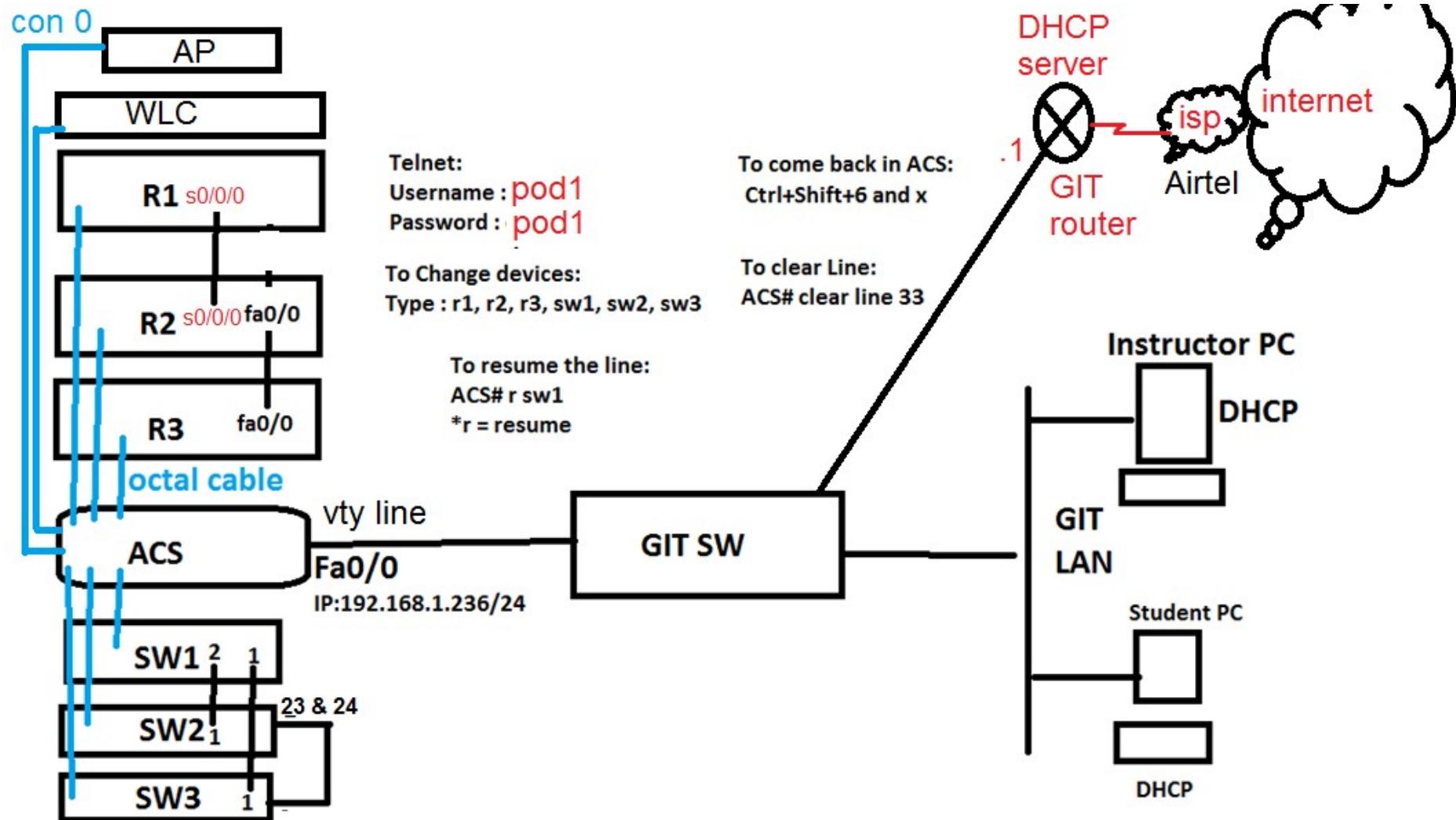
Lesson 29



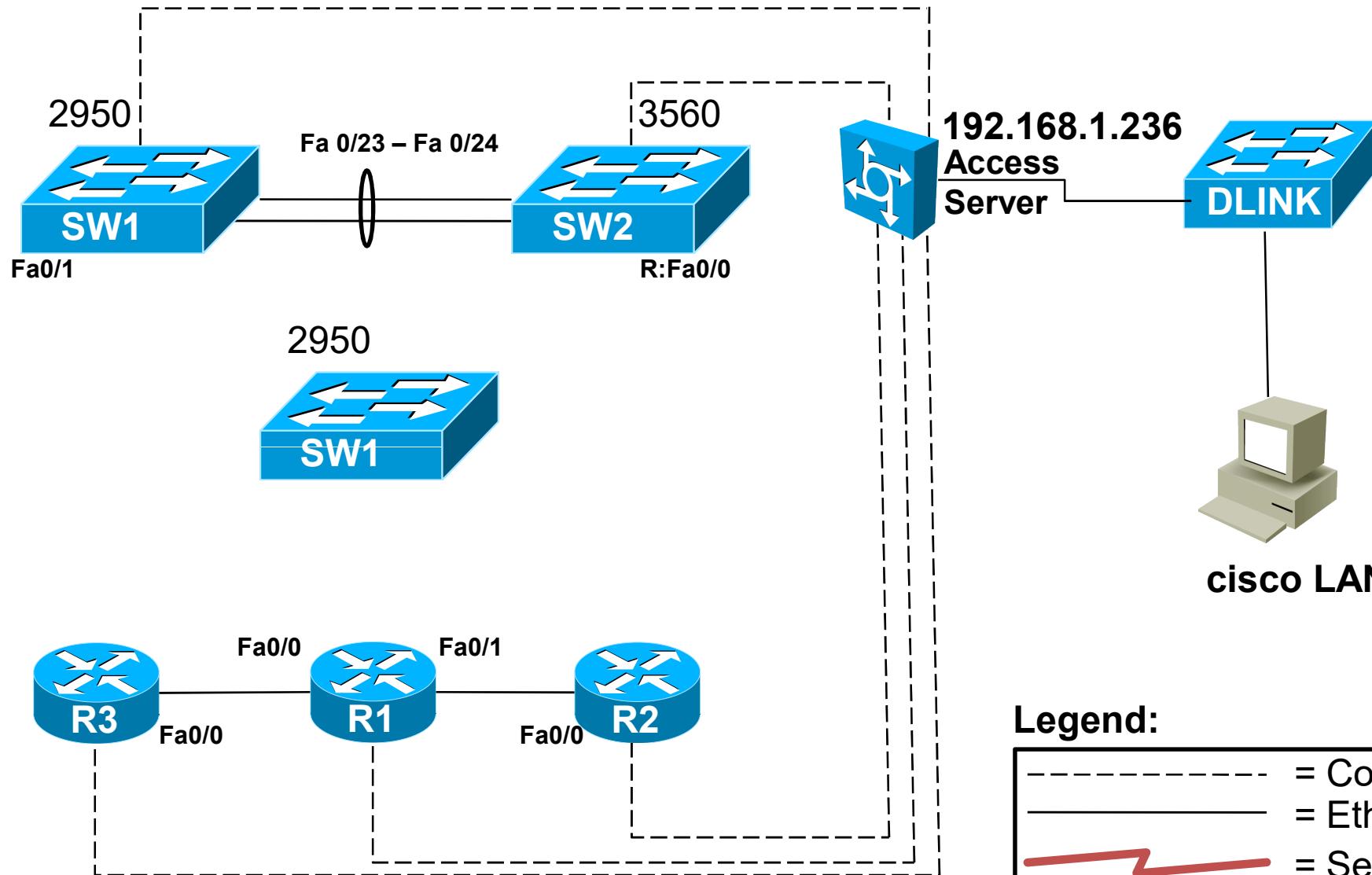
LLDP - Concepts

0. Topology
1. Host Names
2. Configure LLDP
3. Verify

LLDP - Topology



LLDP - Topology



213

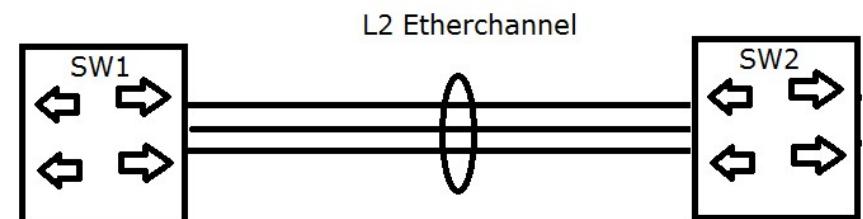
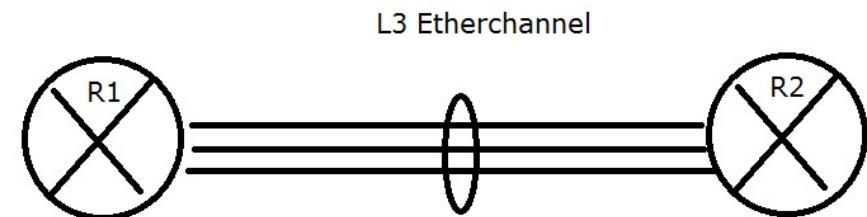
LLDP - Commands

- To verify:
 - SW1# show lldp neighbors

- To change from lldp
 - SW1(config)# no lldp run

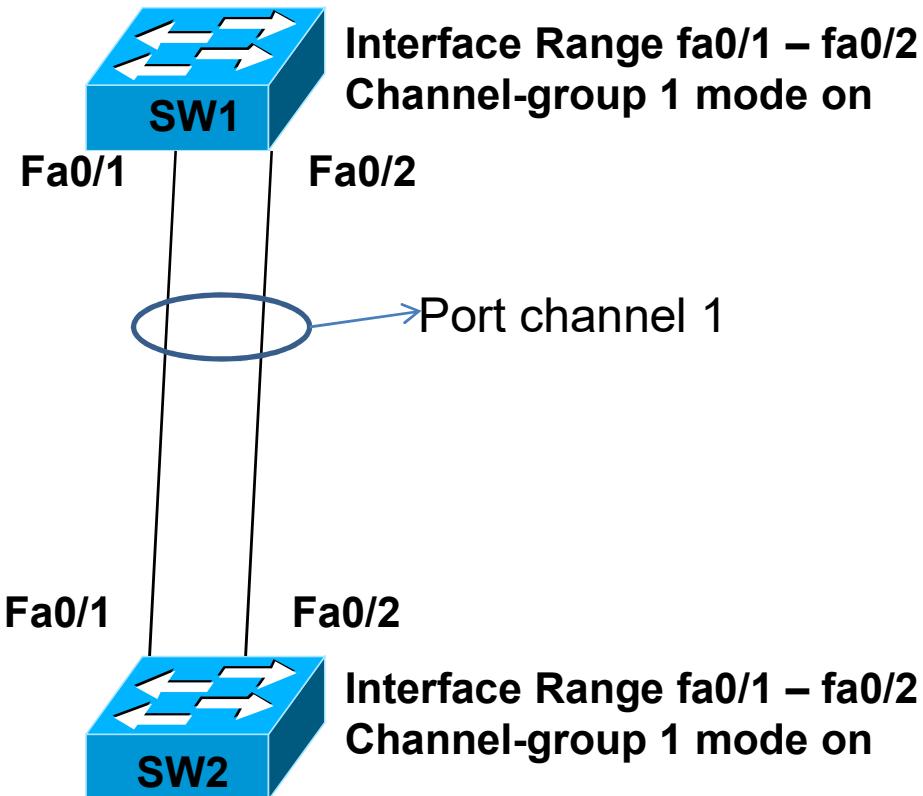
LAN Switching Technologies

L2 - Ether Channel- Static



Ether channel - static

Concept/Topology/Commands



*** Bundling the Ethernet ports & Increasing the bandwidth of uplink

To Verify:

SW1# show etherchannel summary
SW1# show ip interface brief
SW1# show interface port-channel 1



LAN Switching Technologies

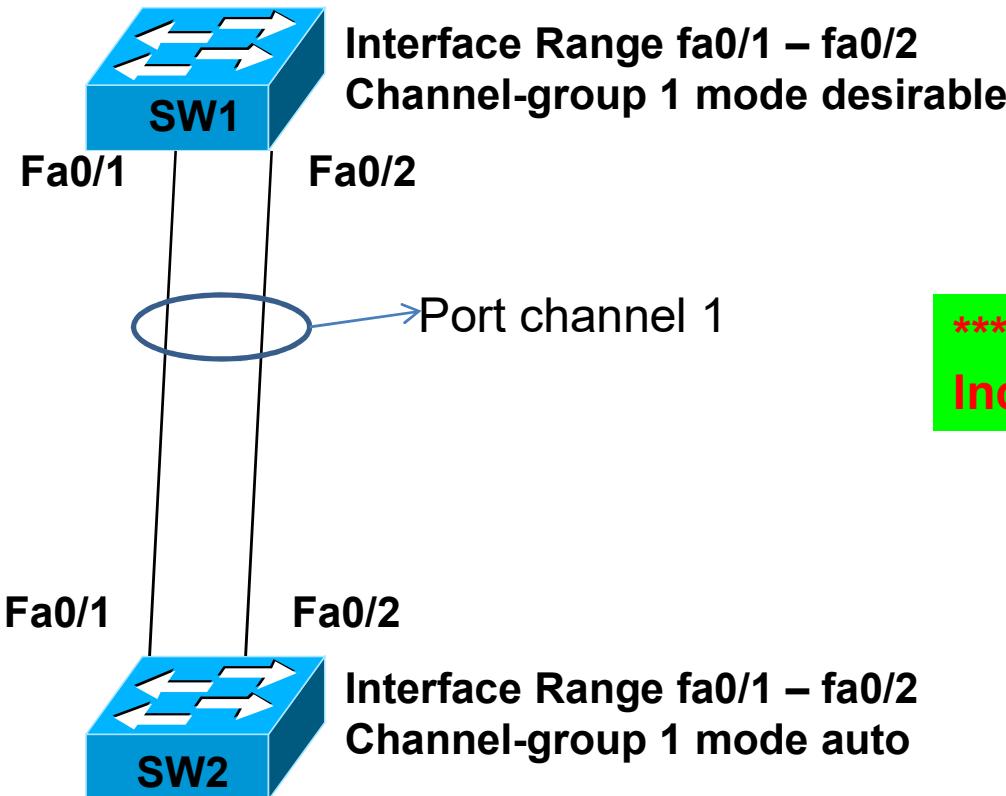
L2 - Ether Channel- Pagg

Lesson 30



Ether channel - PAGP

Concept/Topology/Commands



*** Bundling the Ethernet ports & Increasing the bandwidth of uplink

To Verify:
SW1# show etherchannel summary
SW1# show ip interface brief
SW1# show interface port-channel 1

LAN Switching Technologies

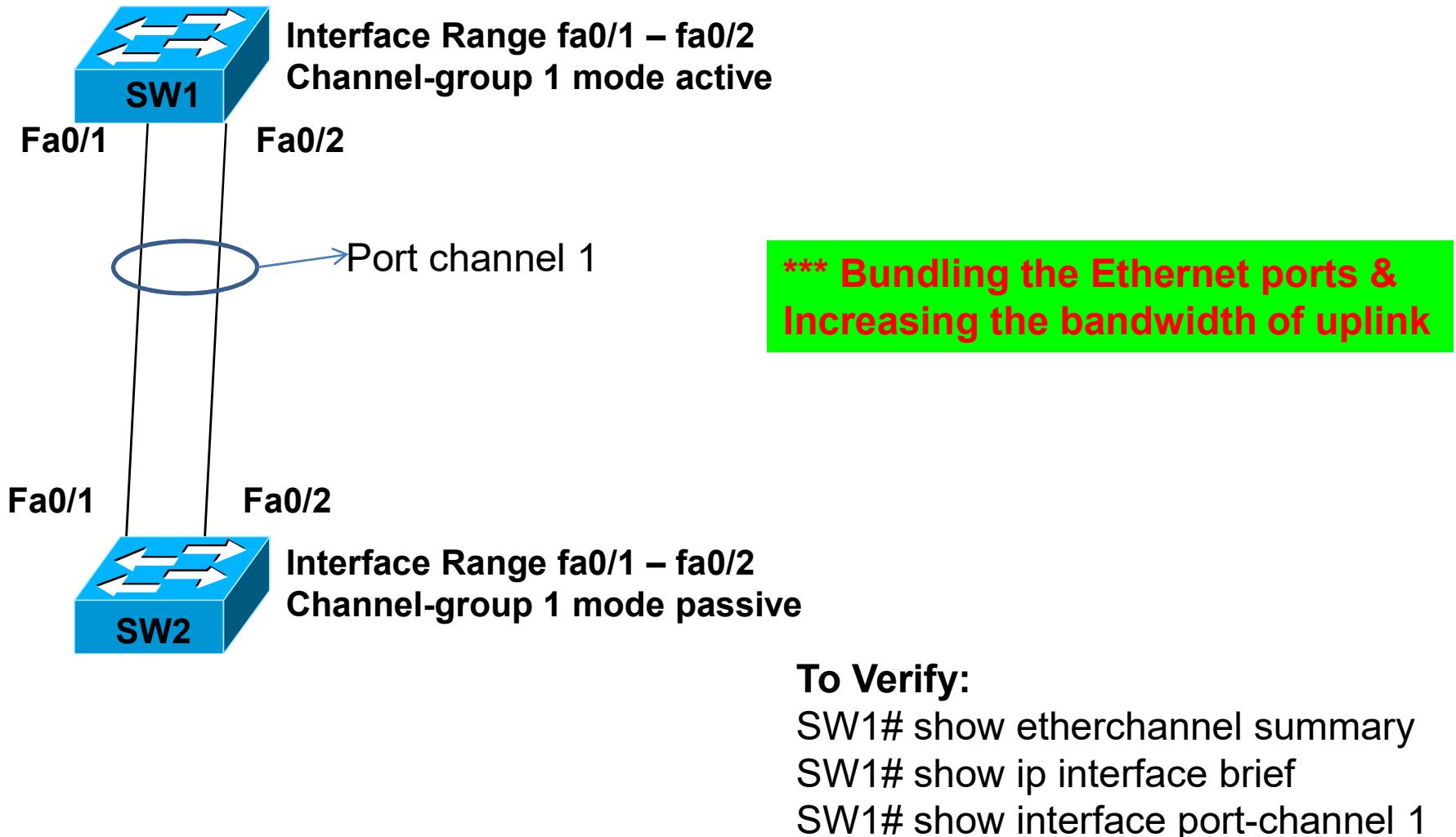
L2 - Ether Channel- LACP

Lesson 30



Ether channel - LACP

Concept/Topology/Commands



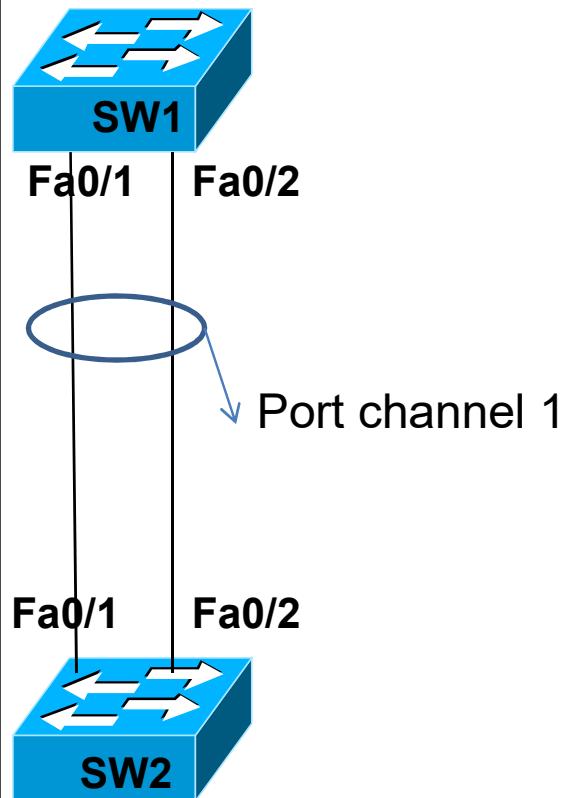
LAN Switching Technologies

L3 - Ether Channel- Static

Lesson 30



L3 Ether channel – Static Concept/Topology/Commands



Create Port channel interface:

```
SW1(config)# interface port-channel 1
SW1(config-if)# no switchport
SW1(config-if)# ip address 192.168.10.1 255.255.255.0
SW1(config-if)# end
```

Configure Physical Interface:

```
SW1(config)# interface range fa 0/1 – fa0/2
SW1(config-if-range)# no ip address {optional}
SW1(config-if-range)# no switchport
SW1(config-if-range)# channel-group 1 mode on
SW1(config-if-range)# end
```

***** Bundling the Ethernet ports & Increasing the bandwidth of uplink**

Create Port channel interface:

```
SW2(config)# interface port-channel 1
SW2(config-if)# no switchport
SW2(config-if)# ip address 192.168.10.2 255.255.255.0
SW2(config-if)# end
```

Configure Physical Interface:

```
SW2(config)# interface range fa 0/1 – fa0/2
SW2(config-if-range)# no ip address {optional}
SW2(config-if-range)# no switchport
SW2(config-if-range)# channel-group 1 mode on
SW2(config-if-range)# end
```

To Verify:

```
SW1# show etherchannel summary
SW1# show ip interface brief
SW1# show interface port-channel 1
```



LAN Switching Technologies

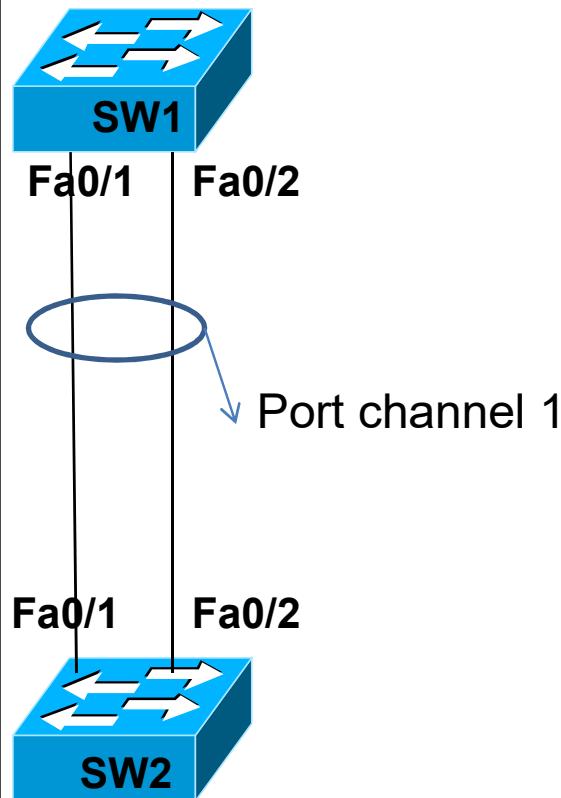
L3 - Ether Channel- PaGP

Lesson 30



L3 Ether channel – PAGP

Concept/Topology/Commands



Create Port channel interface:

```
SW1(config)# interface port-channel 1
SW1(config-if)# no switchport
SW1(config-if)# ip address 192.168.10.1 255.255.255.0
SW1(config-if)# end
```

Configure Physical Interface:

```
SW1(config)# interface range fa 0/1 – fa0/2
SW1(config-if-range)# no ip address {optional}
SW1(config-if-range)# no switchport
SW1(config-if-range)# channel-group 1 mode desirable
SW1(config-if-range)# end
```

***** Bundling the Ethernet ports & Increasing the bandwidth of uplink**

Create Port channel interface:

```
SW2(config)# interface port-channel 1
SW2(config-if)# no switchport
SW2(config-if)# ip address 192.168.10.2 255.255.255.0
SW2(config-if)# end
```

Configure Physical Interface:

```
SW2(config)# interface range fa 0/1 – fa0/2
SW2(config-if-range)# no ip address {optional}
SW2(config-if-range)# no switchport
SW2(config-if-range)# channel-group 1 mode auto
SW2(config-if-range)# end
```

To Verify:

```
SW1# show etherchannel summary
SW1# show ip interface brief
SW1# show interface port-channel 1
```



LAN Switching Technologies

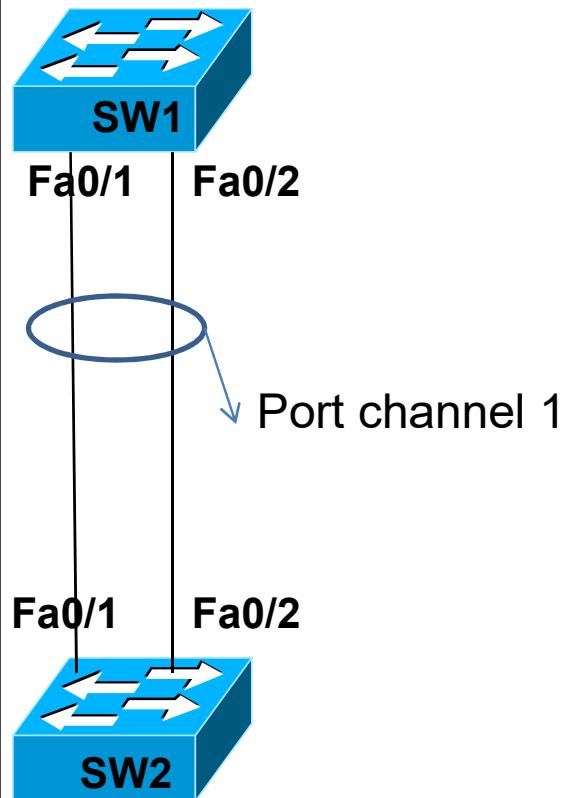
L3 - Ether Channel- LACP

Lesson 30



L3 Ether channel – LACP

Concept/Topology/Commands



Create Port channel interface:

```
SW1(config)# interface port-channel 1
SW1(config-if)# no switchport
SW1(config-if)# ip address 192.168.10.1 255.255.255.0
SW1(config-if)# end
```

Configure Physical Interface:

```
SW1(config)# interface range fa 0/1 – fa0/2
SW1(config-if-range)# no ip address {optional}
SW1(config-if-range)# no switchport
SW1(config-if-range)# channel-group 1 mode active
SW1(config-if-range)# end
```

*** Bundling the Ethernet ports & Increasing the bandwidth of uplink

Create Port channel interface:

```
SW2(config)# interface port-channel 1
SW2(config-if)# no switchport
SW2(config-if)# ip address 192.168.10.2 255.255.255.0
SW2(config-if)# end
```

Configure Physical Interface:

```
SW2(config)# interface range fa 0/1 – fa0/2
SW2(config-if-range)# no ip address {optional}
SW2(config-if-range)# no switchport
SW2(config-if-range)# channel-group 1 mode passive
SW2(config-if-range)# end
```

To Verify:

```
SW1# show etherchannel summary
SW1# show ip interface brief
SW1# show interface port-channel 1
```

Routing Technologies

Inter-VLAN routing

Router on Stick

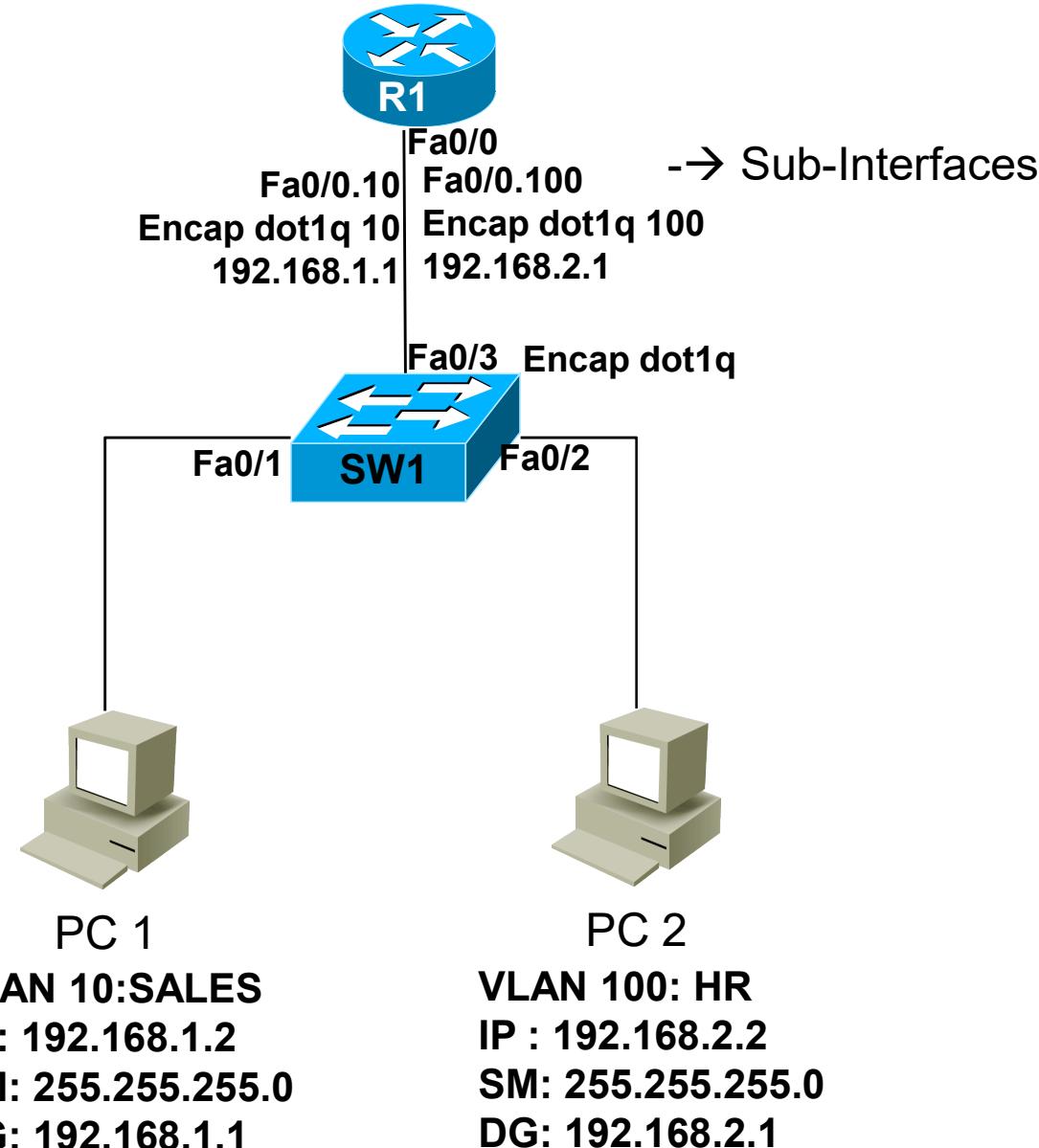
Lesson 31



Router on Stick - Concepts

0. Topology
1. Host Names
2. IP address i.e. PC
3. SW1:Configure VLANS
4. SW1: Assign ports to the VLANS
5. SW1: Configure Trunk
6. R1: Configure sub-interfaces
7. R1: Encapsulation with dot1q & assign VLAN No.
8. R1: Configure IP Address
9. Verify :
 1. Ping PC1 -> PC2

Router on Stick- Topology



Router on Stick - Commands

- To config sub interfaces:
 - R1# configure terminal
 - R1(config)# interface fastEthernet 0/0.10
 - R1(config-subif)# encapsulation dot1q 10
 - R1(config-subif)# ip address 192.168.1.1 255.255.255.0
- To config main interface:
 - R1(config)# interface fastEthernet 0/0
 - R1(config-if)#no shutdown
- To verify:
 - R1# show ip interface brief
 - R1# show running-config
 - PC1:CMD>ping 192.168.2.2
 - PC2:CMD>ping 192.168.1.2

Routing Technologies

Inter-VLAN routing/ L3 Switching

Lesson 32



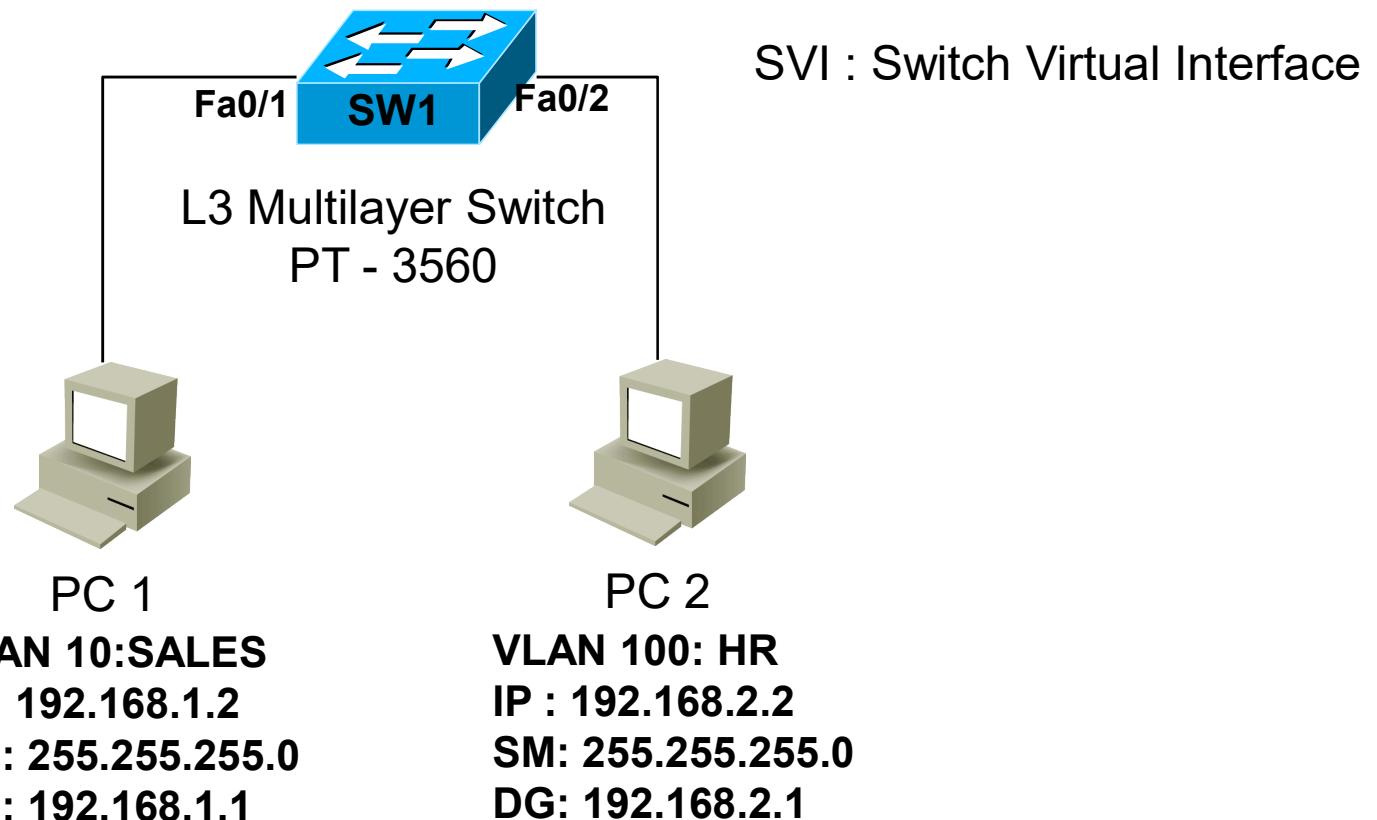
L3 switching - Concepts

0. Topology
1. Host Names
2. IP address
3. SW1:Configure VLANS
4. SW1: Assign ports to the VLANS
5. SW1: Enable routing service
6. SW1: Configure VLAN interfaces i.e. SVI
7. SW1: Configure IP Address in VLAN Interface
8. Verify :
 1. Ping PC1 -> PC2

L3 Switching- Topology

```
SW1(config)# IP Routing  
SW1(config)# int VLAN 10  
SW1(config)# ip address 192.168.1.1 255.255.255.0
```

```
SW1(config)# int VLAN 100  
SW1(config)# ip address 192.168.2.1 255.255.255.0
```



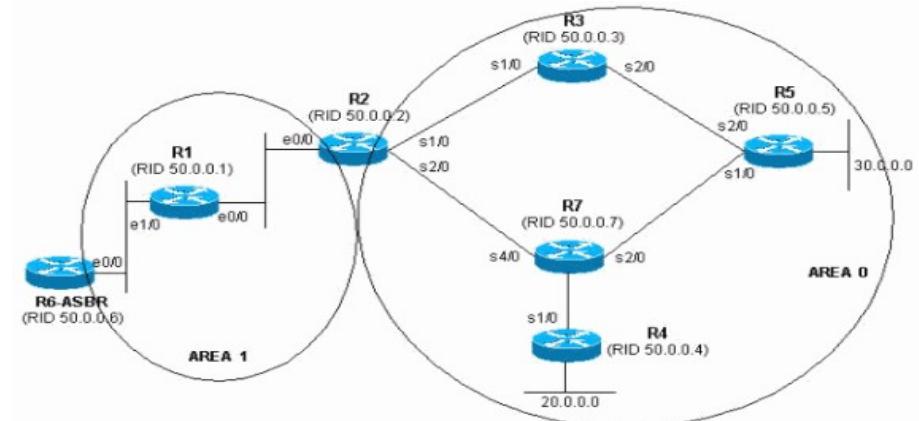
L3 Switching - Commands

- To enable routing services:
 - SW1(config)# ip routing
- To configure vlan interfaces:
 - SW1(config)# interface vlan 10
 - SW1(config-if)# ip address 192.168.1.1 255.255.255.0
 - SW1(config-if)# exit
 - SW1(config)# interface vlan 100
 - SW1(config-if)# ip address 192.168.2.1 255.255.255.0
 - SW1(config-if)# exit
- To verify:
 - SW1# show ip interface brief

Routing Technologies

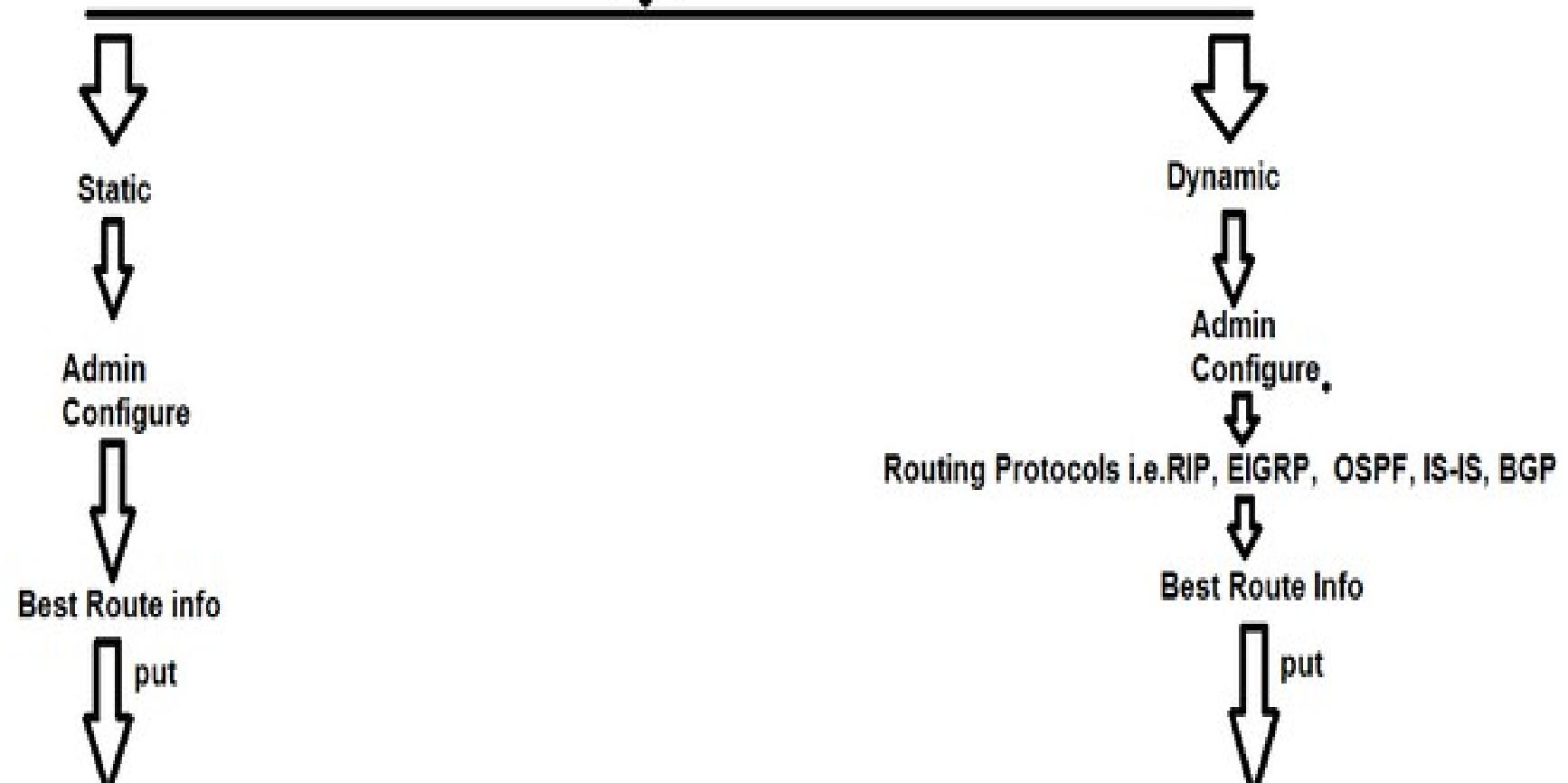
Basics

Lesson 10



What is Routing?

Routing > Selecting the best path/route



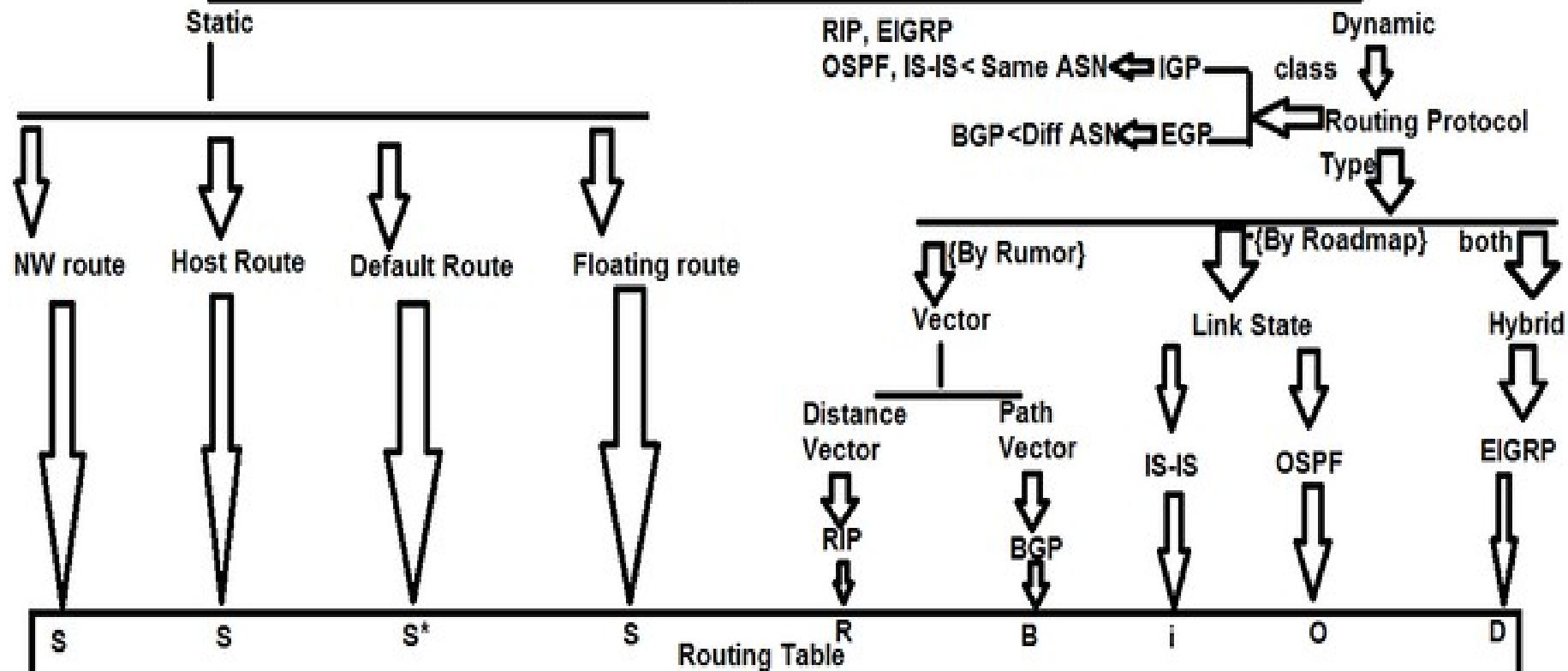
Routing Table Best Route Info:

Destination NW add:Next Hop ip / exit interface
192.168.30.0/24:192.168.20.2 / R1:S0/0/0



Types of Routing

Country = Autonomous System



Source code: C

R1#show ip route

↑ Directly connected interface route



kumar6009@gmail.com

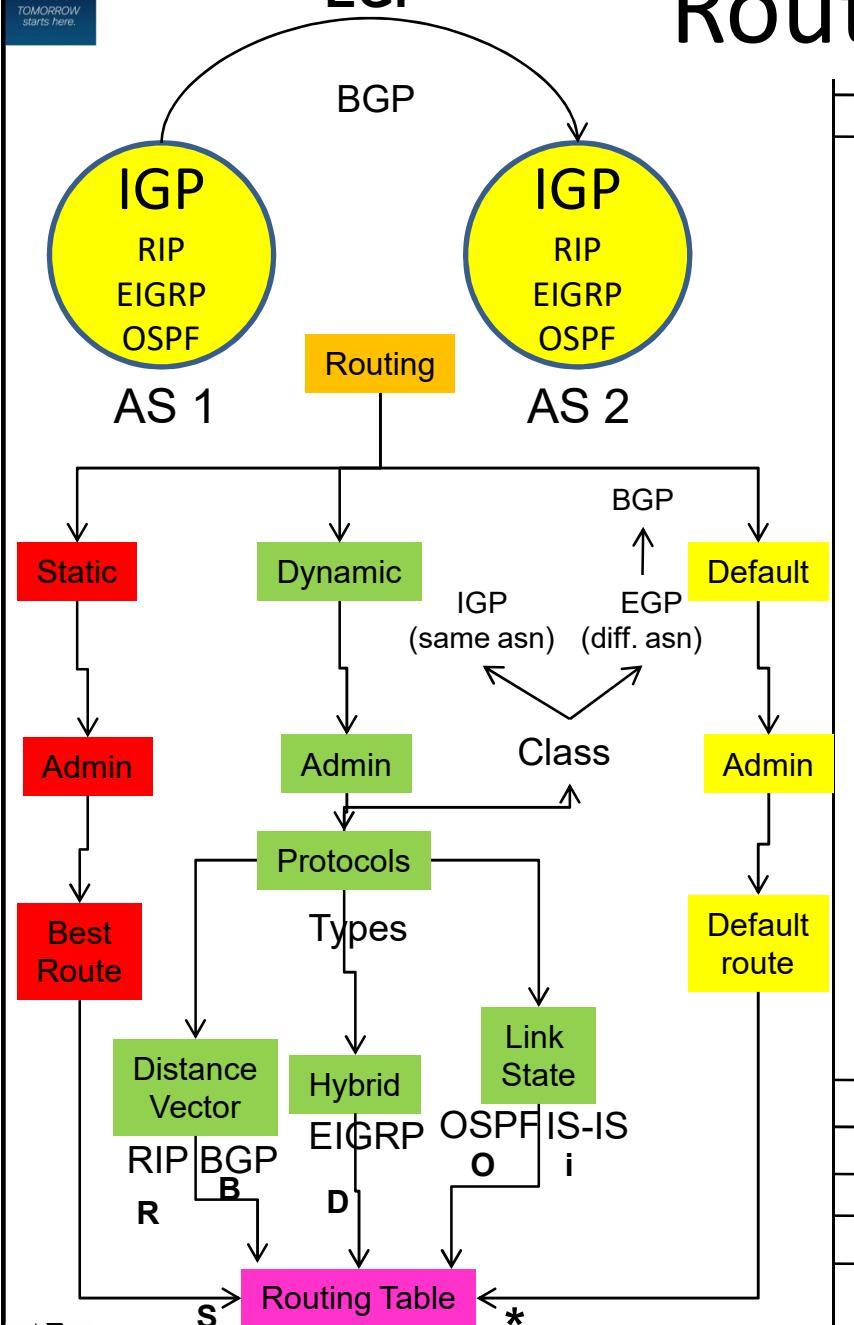


@air.ds2

Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3

Router - Intro

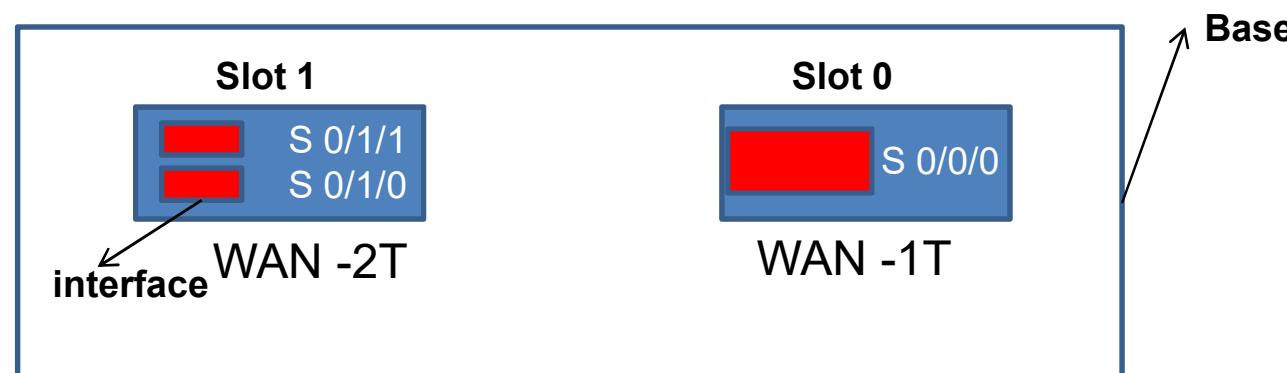
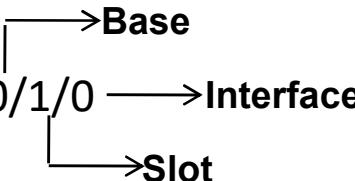


- Layer 3 Device
- Works on Logical Addresses
 - Internet Protocol – Microsoft , Cisco
 - Internet Package exchange {IPX - Novel {First NOS}}
 - AppleTalk – Macintosh – MAC
- **Routed Protocol i.e. logical addressing**
 - IPv4, IPv6, IPX, AppleTalk
- **Routing Protocol i.e. path determination**
 - Distance Vector protocol [routing by rumor]
 - RIP & BGPv4 – Routing information protocol
 - Link state protocol {routing by road map}
 - OSPF – Open Shortest Path First
 - Hybrid Protocol {best of both}
 - EIGRP – Enhanced Interior Gateway Routing Protocol
- Interior Gateway Protocol {Same Autonomous System}
 - RIPv1, RIPv2, OSPF & EIGRP
- Exterior Gateway Protocol {Different Autonomous System}
 - BGPv4 – Border Gateway Protocol
- Connects different logical Networks i.e. subnets
- Select best path
- Routing {Routing Table & Switching/Forwarding [ARP Table]}
- Connects LAN-WAN
- Maintains Routing Table

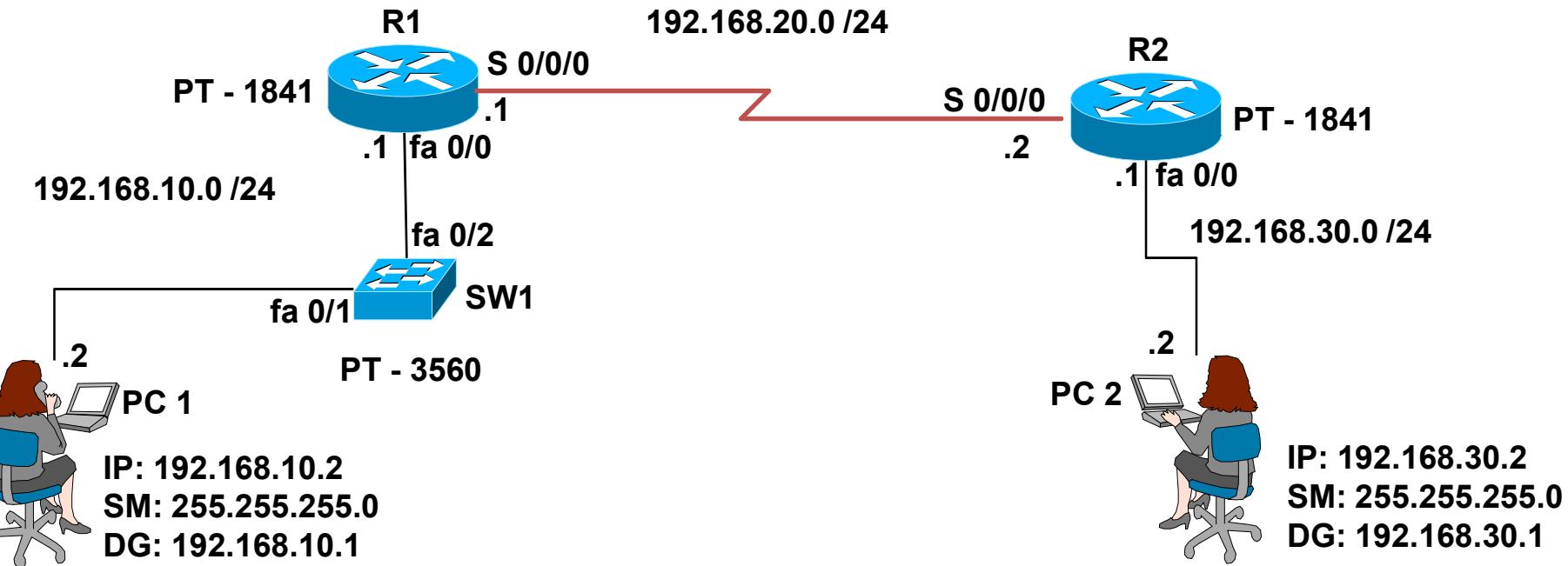
Router Configuration - Interfaces

- Router Interfaces i.e. All Interface Numbers starts from “0”

- LAN Interfaces
 - Ethernet: e0, e1, e2, e0/0, e0/1
 - Fast Ethernet: fa0/0, fa0/1, fa0/2, fa0/0/0, fa0/1/1
 - Gigabit Ethernet: G0/0, G0/1
- WAN Interfaces
 - Serial : S0/0, S0/1, S 0/0/0, S 0/1/0
 - E1/T1 Ports



Interpret a Network Diagram



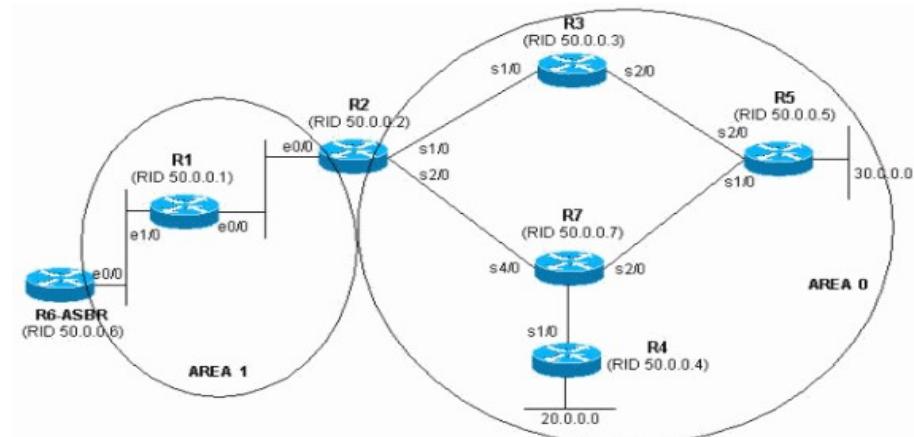
Exercise:

- IP address
- No. of Networks
- Network Address
- Directly connect Network Address: via which interface (R1, R2)
- Destination Network Address: via Next hop IP / Exit Interface

Routing Technologies

Serial {WAN}

Lesson 13

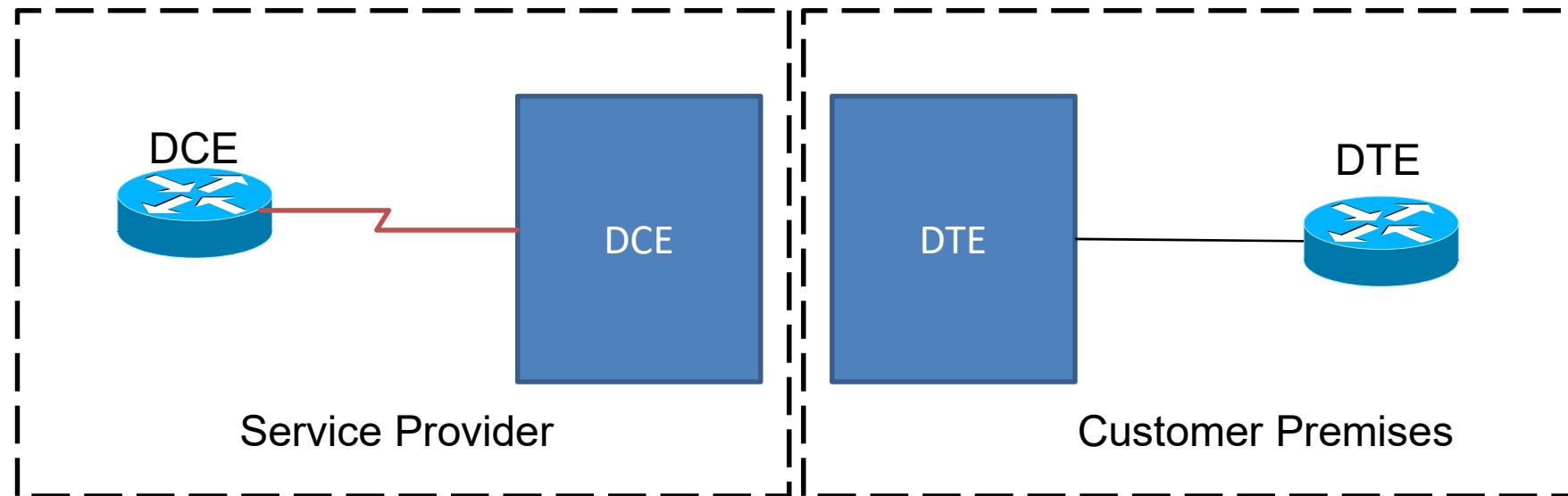


Serial - Concepts

0. Topology
1. Host Name
2. IP address i.e. PC1, PC2, R1, R2
3. Serial config
 1. Find DCE/DTE
 2. Config:
 1. DCE: clock rate 64000
4. Ping
 1. PC1 -> PC2
 2. PC2 -> PC1
5. Understand
 1. Different ping replies
 1. Request Timed out {R}
 2. Destination Host Unreachable {U}
 3. Reply {!}
 4. No Reply {.}



Router Configuration – Serial config

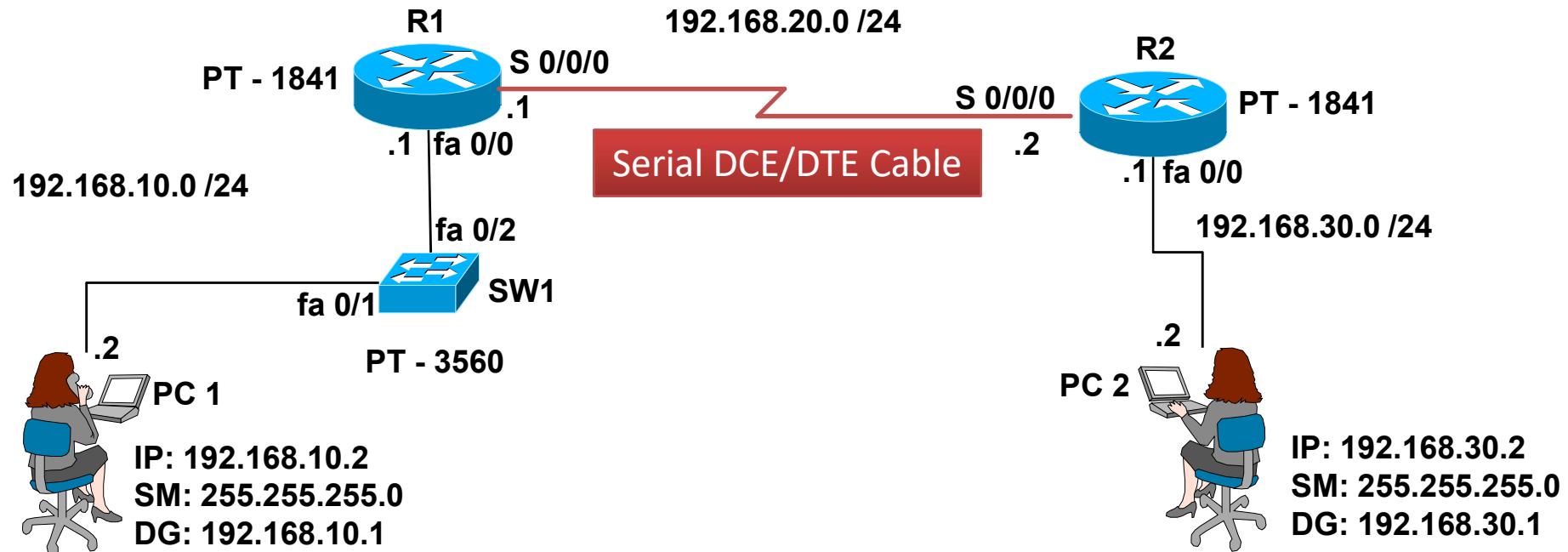


DCE: Data Communication Equipment {Service Provider End}

DTE: Data Terminal Equipment {User End}

*** Clock Rate is always in DCE i.e. Service Provider end

Lab 13[serial] to Lab18[RIP] - Topology



- IPconfig & Trouble shooting
 - Router> enable
 - Router# configure terminal
 - Router(config)# hostname R1
 - R1(config)#Interface fa 0/0
 - R1(config-if)#ip address 192.168.10.1 255.255.255.0
 - R1(config-if)#no shutdown
 - R1(config-if)#exit
 - R1(config)#

Router Configuration – Serial config

- IPconfig & Trouble shooting
 - R1(config)#Interface S 0/0/0
 - R1(config-if)#ip address 192.168.20.1 255.255.255.0
 - R1(config-if)#no shutdown
 - R1(config-if)#exit
 - R1(config)#exit
 - R1#ping 192.168.10.1
 - R1#ping 192.168.20.1
- Router 2: IPconfig & Trouble shooting
 - Router> enable
 - Router# configure terminal
 - Router(config)# hostname R2
 - R2(config)#Interface fa 0/0
 - R2(config-if)#ip address 192.168.30.1 255.255.255.0
 - R2(config-if)#no shutdown
 - R2(config-if)#exit
 - R2(config)#
 - R1(config)#Interface S 0/0/0
 - R1(config-if)#ip address 192.168.20.2 255.255.255.0
 - R1(config-if)#no shutdown
 - R1(config-if)#exit
 - R1(config)#exit
 - R1#ping 192.168.30.1
 - R1#ping 192.168.20.2



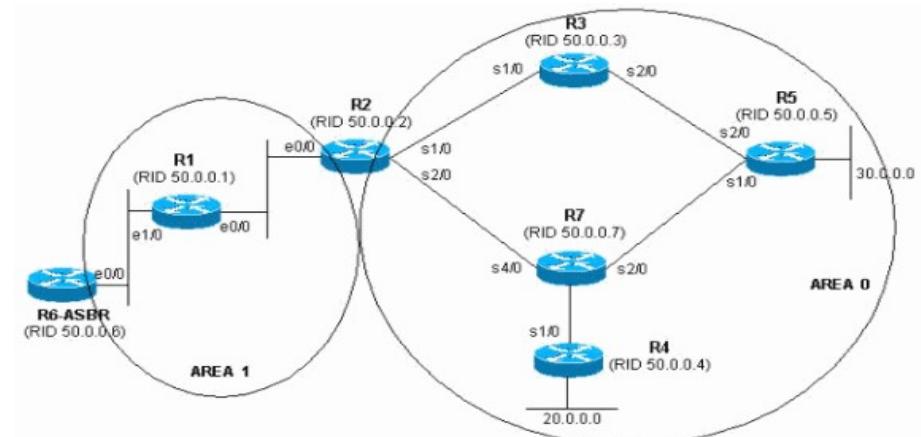
Router Configuration – Serial config

- **Clock rate - IPconfig & Trouble shooting**
 - R1(config)#Interface S 0/0/0
 - R1(config-if)#clock rate 64000 {bits per second}
 - R1(config-if)#exit
 - R1(config)#exit
- **To Verify DCE/DTE:**
 - R1#show controllers S 0/0/0
- **To Verify Interface ip address, L1 & L2 status:**
 - R1# show ip interface brief

Routing Technologies

Static Routing

Lesson 14



Static - Routing

- **Routing**

- **Static Routing i.e. Manually**
- **Dynamic Routing i.e. RIP, EIGRP & OSPF {Routing Protocols}**
- **Default Routing**
 - Single route
 - Single exit point
 - Stub network

Pros:

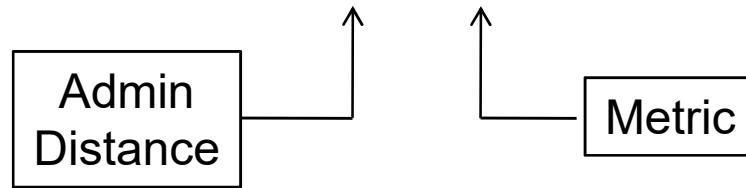
- Bandwidth
- Security
- Less per head i.e. CPU
- AD Administrative Distance {1}

Cons:

- No Auto Update
- Small networks

R1#show ip route

D 172.30.10.0 [90/20514560] via 10.1.24.2, 00:05:45, Serial0/0/0

**Administrative Distance:**

Trust Worthiness of the Route

Number – 0 to 255

Lesser the number, more the trust

AD No.	Routes
0	Directly connected
1	static
90	EIGRP
110	OSPF
120	RIP
255	unknown



Static - Routing

R1#show ip route

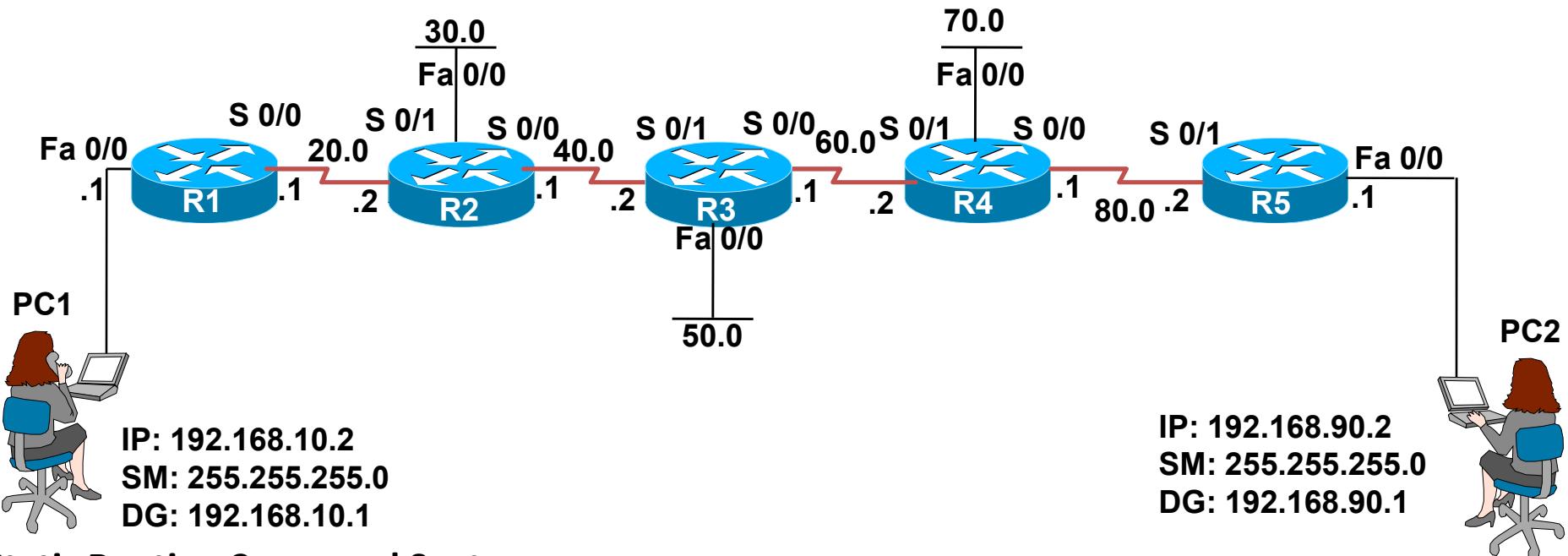
D 172.30.10.0 [90/20514560] via 10.1.24.2, 00:05:45, Serial0/0/0

- D = Source of the Route i.e. D = EIGRP Route
- 172.30.10.0 = Destination Network Address
- 90 = Admin Distance
 - Parameter to select the best source of route
- 20514560 = Metric i.e. Parameter to select the best route
- 10.1.24.2 = Next Hop IP Address
- 00:05:45 = Duration i.e. HH:MM:SS
- Serial0/0/0 = Exit Interface

A **Gateway of Last Resort** or Default **gateway** is a route used by the router when no other known route exists to transmit the IP packet. Known routes are present in the routing table.



Static Routing Exercise



Static Routing Command Syntax:

R1(config)#ip route [Destination Network subnet mask] [Next Hop Ip address/Exit Interface]

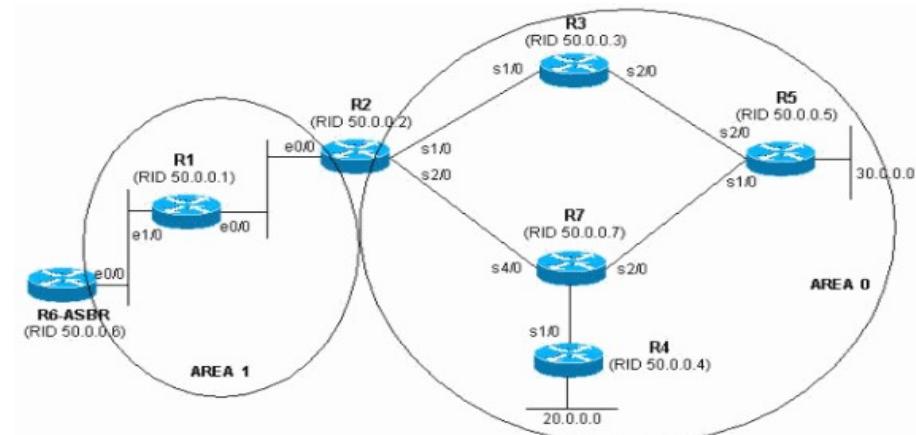
```
R3(config)#ip route 192.168.10.0 255.255.255.0 192.168.40.1
R3(config)#ip route 192.168.20.0 255.255.255.0 192.168.40.1
R3(config)#ip route 192.168.30.0 255.255.255.0 192.168.40.1
```

```
R3(config)#ip route 192.168.70.0 255.255.255.0 192.168.60.2
R3(config)#ip route 192.168.80.0 255.255.255.0 192.168.60.2
R3(config)#ip route 192.168.90.0 255.255.255.0 192.168.60.2
```

Routing Technologies

Static - Host Route

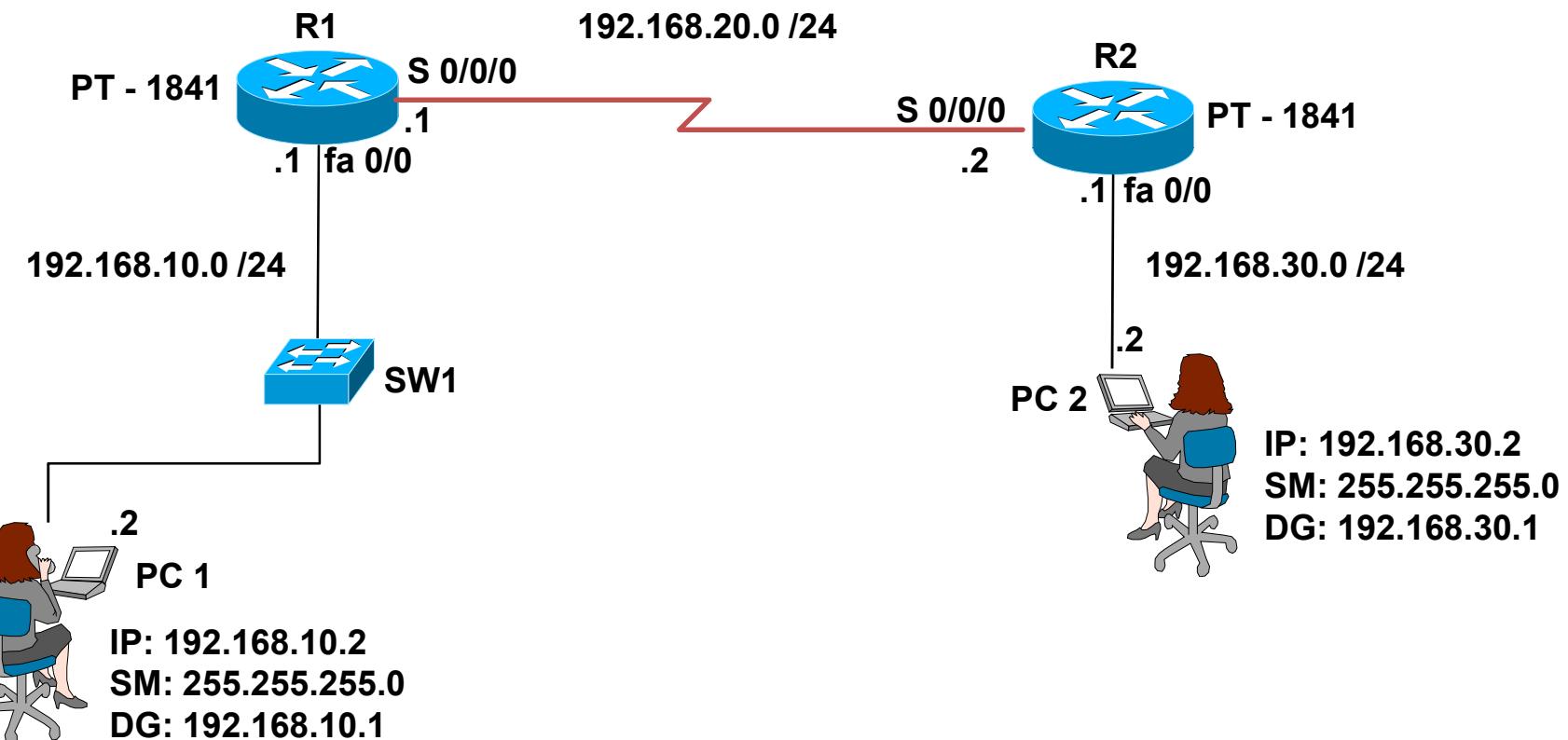
Lesson 14



Static - Concepts

- 0. Topology**
- 1. Host Name**
- 2. IP address i.e. PC1, PC2, R1, R2**
- 3. Serial config**
 - 1. Find DCE/DTE**
 - 2. Config:**
 - 1. DCE: clock rate 64000**
- 4. Ping**
 - 1. PC1 -> PC2**
 - 2. PC2 -> PC1**
- 5. Configure Static - Host Command**
- 6. Verify in Routing Table {C& S}**
- 7. Ping**
 - 1. PC1 -> PC2**
 - 2. PC2 -> PC1**

Static - Topology



Static - Commands

- Syntax:

Router(config)#ip route [Destination Host Address subnet mask] [Next Hop Ip address/Exit Interface]

- To configure static:

R1:

- R1(config)# ip route 192.168.30.2 255.255.255.255 192.168.20.2

R2:

- R2(config)# ip route 192.168.10.2 255.255.255.255 192.168.20.1

- To verify:

- R1# show ip route {In routing table a route with “S” will be added.

- Ping

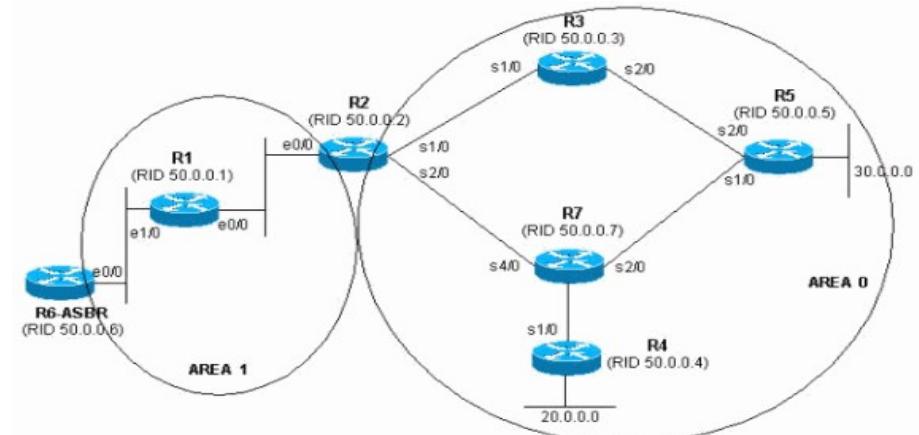
- PC1 -> PC2
 - PC2 -> PC1



Routing Technologies

Static - Network Route

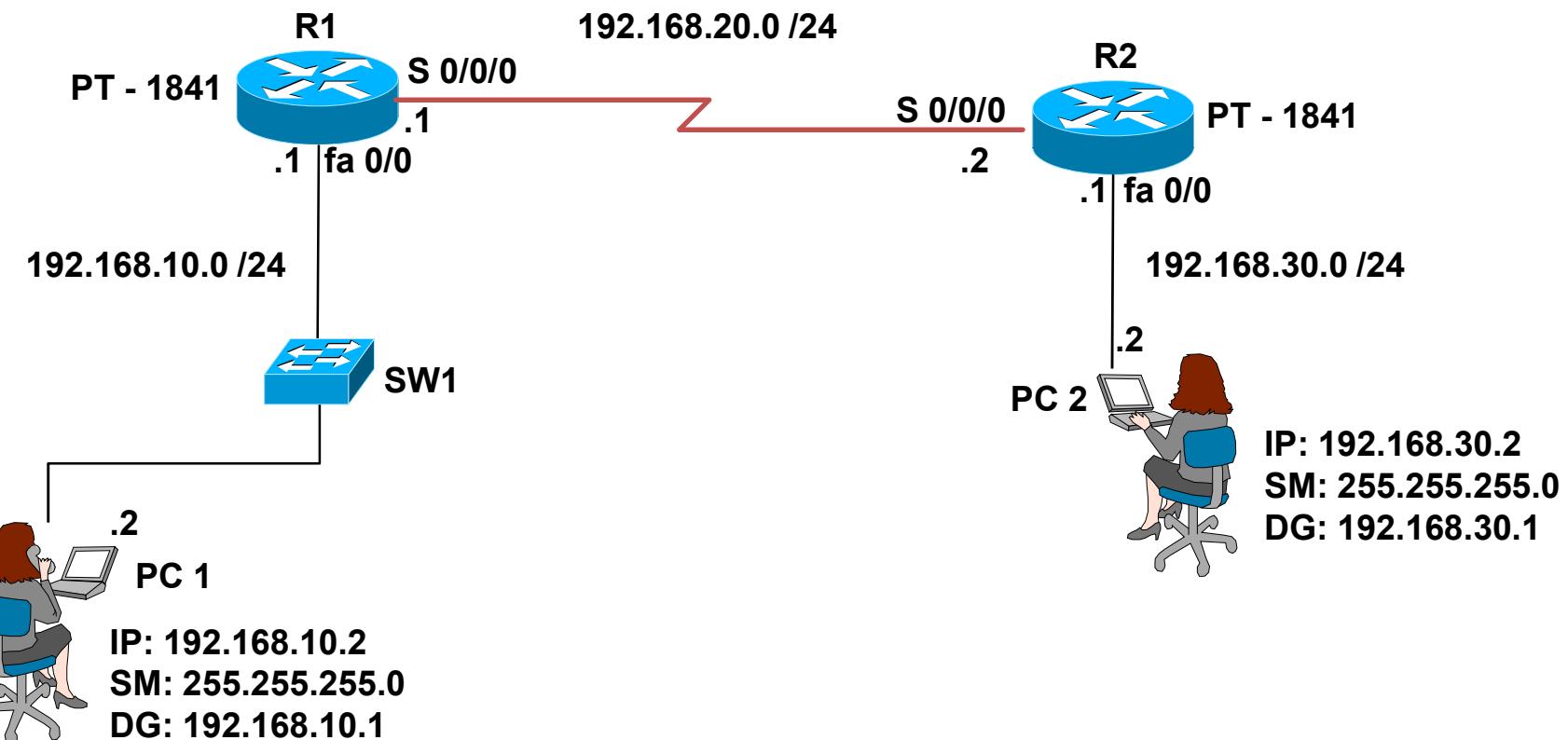
Lesson 14



Static - Concepts

- 0. Topology**
- 1. Host Name**
- 2. IP address i.e. PC1, PC2, R1, R2**
- 3. Serial config**
 - 1. Find DCE/DTE**
 - 2. Config:**
 - 1. DCE: clock rate 64000**
- 4. Ping**
 - 1. PC1 -> PC2**
 - 2. PC2 -> PC1**
- 5. Configure Static –Network route command**
- 6. Verify in Routing Table {C& S}**
- 7. Ping**
 - 1. PC1 -> PC2**
 - 2. PC2 -> PC1**

Static - Topology



Static - Commands

- Syntax:

Router(config)#ip route [Destination Network Address subnet mask] [Next Hop Ip address/Exit Interface]

- To configure static:

R1:

- R1(config)# ip route 192.168.30.0 255.255.255.0 192.168.20.2

R2:

- R2(config)# ip route 192.168.10.0 255.255.255.0 192.168.20.1

- To verify:

- R1# show ip route {In routing table a route with “S” will be added.

- Ping

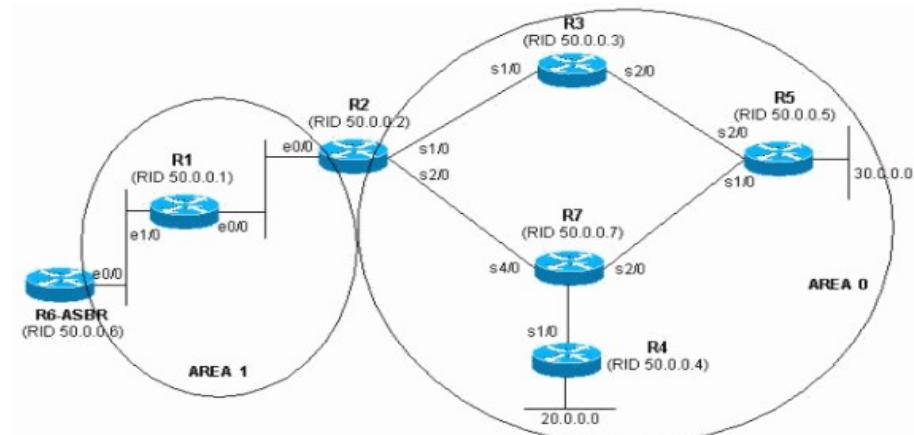
- PC1 -> PC2
 - PC2 -> PC1



Routing Technologies

Static - Default Route

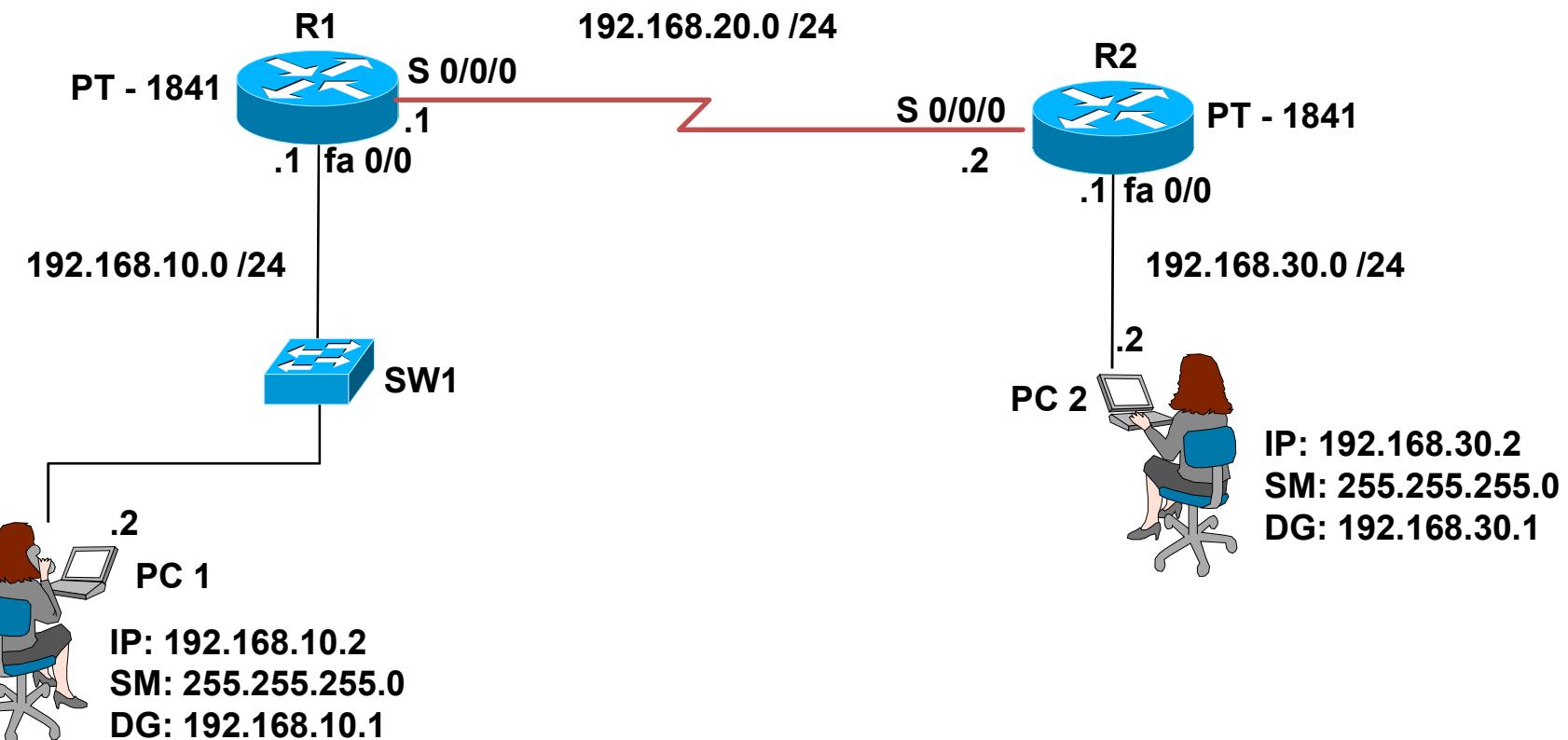
Lesson 14



Static - Concepts

- 0. Topology**
- 1. Host Name**
- 2. IP address i.e. PC1, PC2, R1, R2**
- 3. Serial config**
 - 1. Find DCE/DTE**
 - 2. Config:**
 - 1. DCE: clock rate 64000**
- 4. Ping**
 - 1. PC1 -> PC2**
 - 2. PC2 -> PC1**
- 5. Configure Static - Host Command**
- 6. Verify in Routing Table {C& S}**
- 7. Ping**
 - 1. PC1 -> PC2**
 - 2. PC2 -> PC1**

Static - Topology



Default Routing - Commands

- Syntax:

Router(config)#ip route [Destination Network Address subnet mask] [Next Hop Ip address/Exit Interface]

- To configure static:

R1:

- R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.20.2

R2:

- R2(config)# ip route 0.0.0.0 0.0.0.0 192.168.20.1

- To verify:

- R1# show ip route {In routing table a route with “S*” will be added.

- Ping

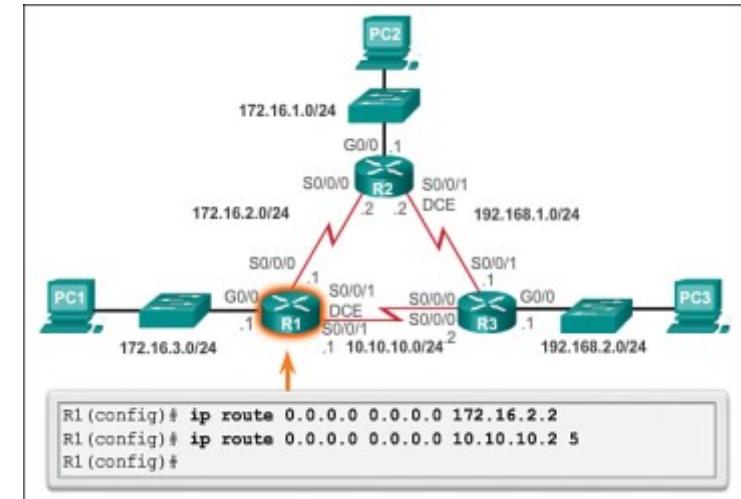
- PC1 -> PC2
 - PC2 -> PC1



Routing Technologies

Static - Floating Route

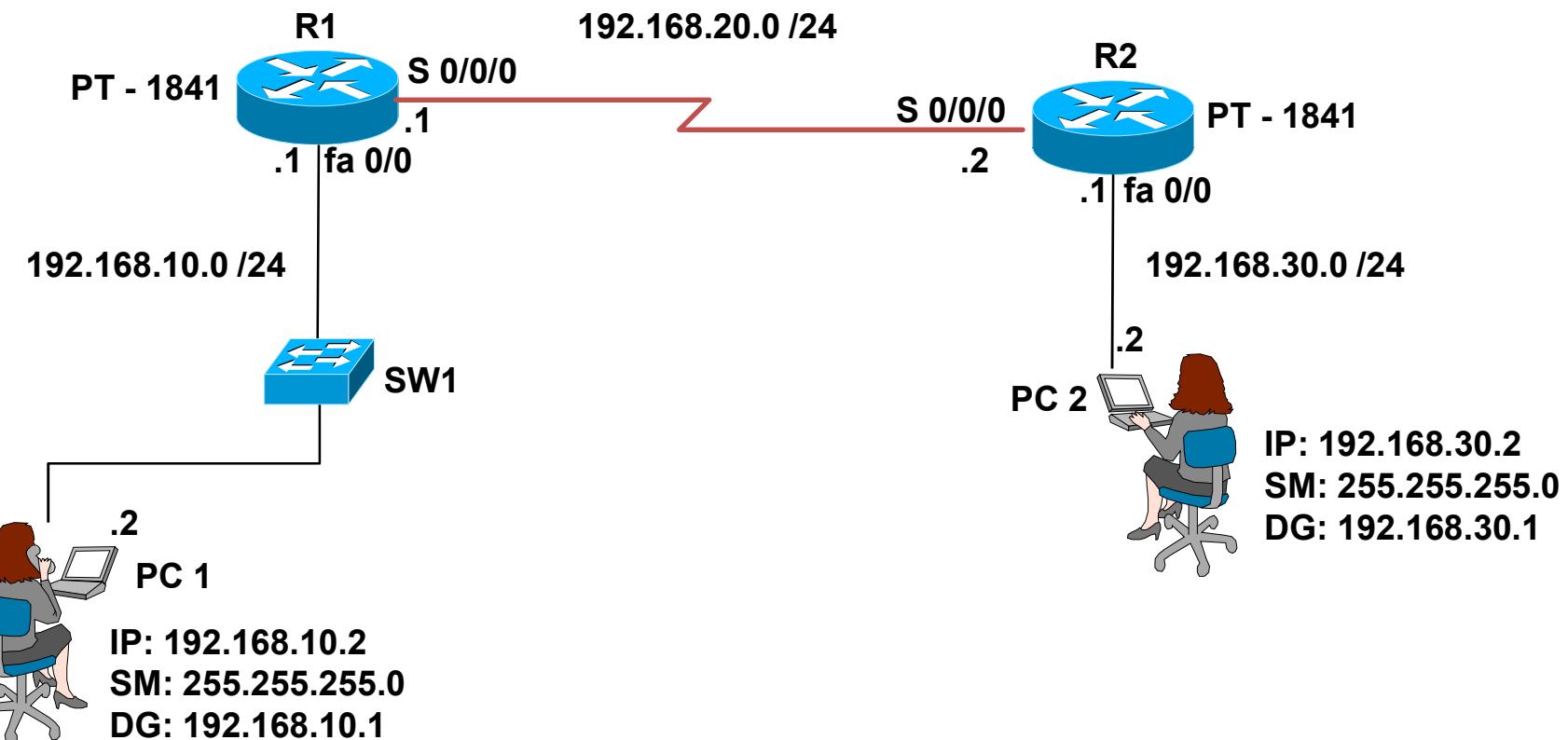
Lesson 14



Static - Concepts

- 0. Topology**
- 1. Host Name**
- 2. IP address i.e. PC1, PC2, R1, R2**
- 3. Serial config**
 - 1. Find DCE/DTE**
 - 2. Config:**
 - 1. DCE: clock rate 64000**
- 4. Ping**
 - 1. PC1 -> PC2**
 - 2. PC2 -> PC1**
- 5. Configure Static - Host Command**
- 6. Verify in Routing Table {C& S}**
- 7. Ping**
 - 1. PC1 -> PC2**
 - 2. PC2 -> PC1**

Static - Topology



Floating Routing - Commands

- Syntax:

```
Router(config)#ip route [Destination Network Address subnet mask] [Next Hop Ip  
address/Exit Interface] [admin Distance]
```

- To configure static:

R1:

- R1(config)# ip route 192.168.30.0 255.255.255.0 192.168.20.2 121

To verify:

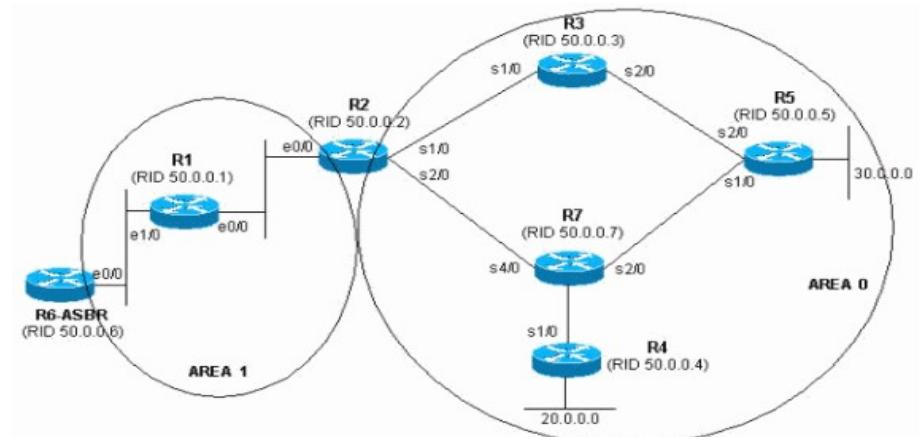
- Disable RIP
- R1# show ip route {In routing table a route with “S with AD 121” will be added.
- Ping
 - PC1 -> PC2
 - PC2 -> PC1



Routing Technologies

RIPv2

Lesson 15



RIP - Concepts

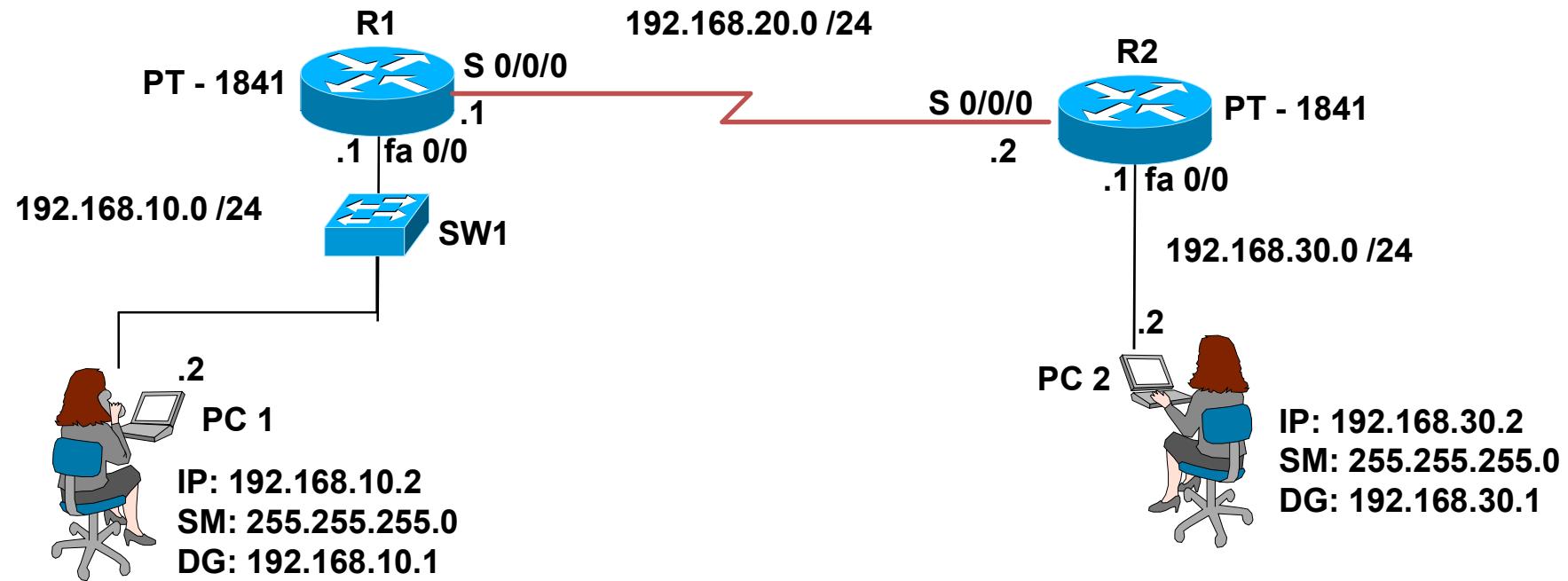
- Distance Vector Protocol
 - Takes routes from neighbors routers and updates its routing table i.e. Routing by Rumor
- IGP i.e. Interior Gateway Protocol
 - Same Autonomous system Number
- Metric
 - Parameter to select the best route
 - HOP count
 - 1 hop count = 1 router
- Timers
 - Update timer : 30 S
 - Invalid timer : 180 S
 - Hold down timer : 180 S
 - Flush timer : 240 S
- Max Hop count = 15

RIP - Concepts

0. Topology
1. Host Names {PT & Hosts}
2. IP address
3. Serial
4. Routing protocols
 1. RIP
 1. Start RIP protocol {Router RIP}
 2. In Router Config mode
 - Network Command i.e. Advertise my directly connected network address
 - » Add Interfaces to Routing Protocol
 3. Version 2 {CIDR, Multicasting & Auth}
5. To Verify
 1. Show ip Route {"R" = RIP}
 2. Ping
 1. PC1 -> PC2
 2. PC2 ->PC1



RIP - Topology



RIP- Commands

- To configure RIP: Configure in R2 also:
 - R1(config)# router rip
 - R1{config-router}# network [directly connected network address i.e. “C” in the Routing table]
 - R1{config-router}# network 192.168.10.0
 - R1{config-router}# network 192.168.20.0
 - R1{config-router}# version 2
 - R1{config-router}# exit

- To verify

R1:

- R1# show ip interface brief
- R1# show running –config
- R1# show ip protocols
- R1# Show ip route

- To see the inside RIP traffic:

- R1# Debug ip rip events

- To stop the debugging

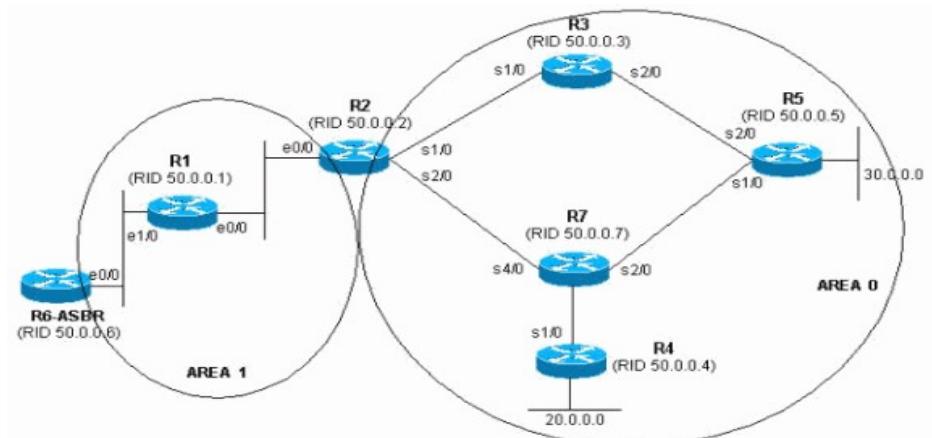
- R1# no debug all



Routing Technologies

EIGRP

Lesson 16



EIGRP Concepts

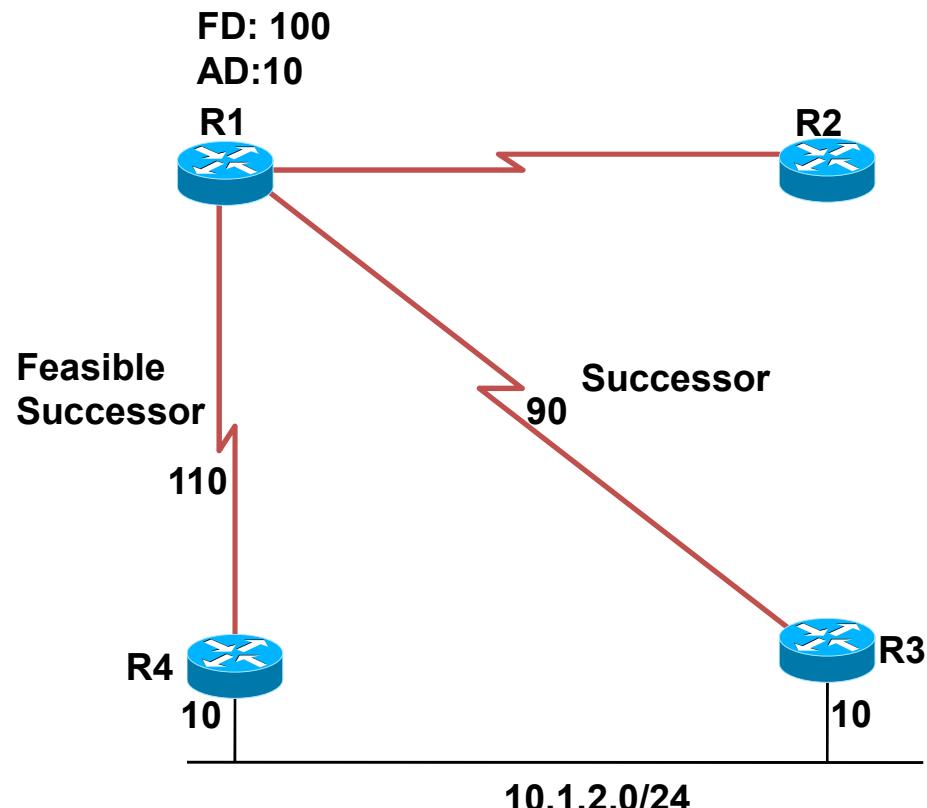
- Enhanced Interior Gateway Routing Protocol
 - Pre-successor = IGRP = Classful Routing Protocol
- Advance D.V. /Hybrid Protocol
- Cisco's proprietary protocol
- Metric = K Value i.e. Default {Bandwidth & Delay}
- Max Hop count: 255 {Default = 100}
- Classless Routing Protocol
 - Configure No Auto-summary - Support CIDR & VLSM
- Before sending updates, It will establish neighborhood
- DUAL
 - Diffuse Update Algorithm
- Table:
 - Neighbor Table {neighbor address}
 - Topology Table {full network details – All routes}
 - Routing Table {Only the Best Routes}



EIGRP Concepts

Terminologies:

1. FD - Feasible Distance
 - Total distance to Destination NW
2. AD - Advertised Distance
 - Next hop's Total distance to Destination NW
3. S –Successor
 - Lower FD – Primary Route
4. FS -Feasible Successor
 - Next Lower FD – Backup route
5. FC - Feasibility Condition
 - AD must less my FD
6. A - Active Route
 - In Topology Table: Route is down
7. P - Passive Route
 - In Topology Table: Route is safe



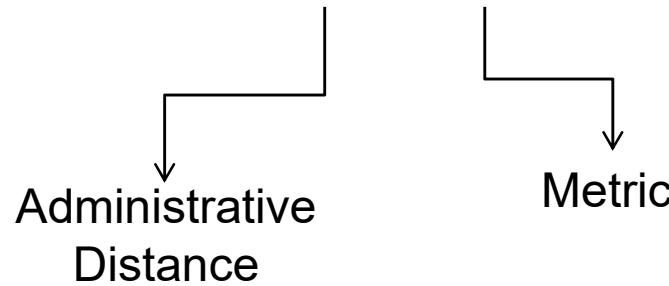
Neighborhood:

- Hello : Forms Relationship
 - Checks – Are you same autonomous system number
- Update: Sending updates
- Query: Ask for Routes
- Reply : Response to a Query
- ACK: Updates, Query & Reply messages



EIGRP Concepts

- Metric Calculation i.e. Parameters to find the best path
 - Default: Bandwidth & Delay {static}
 - On Demand: Load(% of Traffic), Reliability(% of downtime) & MTU {Maximum Transmission Unit i.e. How much data can be send in single packet} – {Dynamic}
 - Complex Formula to find the
 - Composite metric is computed as.... “K Value” i.e. Numbers will in 8 digits
 - Metric = $[k1 * \text{bandwidth} + (k2 * \text{bandwidth}) * (256 - \text{load}) + k3 * \text{delay}]$
 - If $k5 \neq 0$, Metric = $\text{metric} * [k5 / \text{reliability} + k4]$
 - Default K values are $K1=1[\text{bw}]$ $k2=0[\text{load}]$, $k3=1[\text{delay}]$, $k4=0[\text{reliability}]$ & $k5=0[\text{MTU}]$
 - D 172.30.10.0 [90/20514560] via 10.1.24.2, 00:05:45, Serial0/0/0



- **Administrative Distance:**
 - Trust Worthiness of the Route
 - Number – 0 to 255
 - Lesser the number, more the trust

AD No.	Routes
0	Directly connected
1	Static
90	EIGRP
110	OSPF
120	RIP
255	unknown



EIGRP Concepts



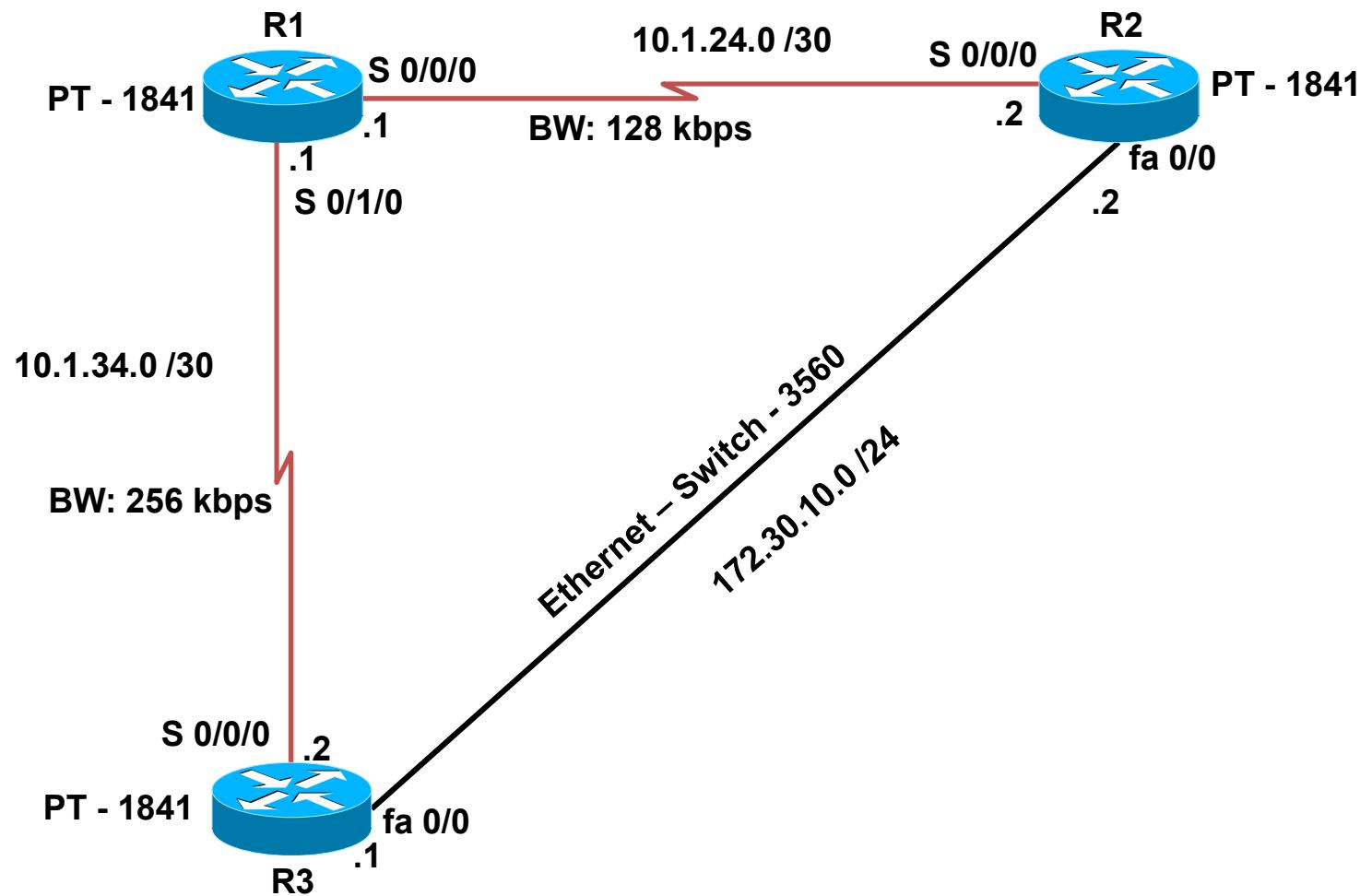
- **Routing Loops**
 - When packet is roaming in the network without reaching the destination is called a loop
- **Routing Loops Prevention Mechanisms**
 1. Maximum Hop count {RIP = 15 hops}
 2. Triggered Update {Not waiting for next periodic update}
 3. Hold down Timer {Dead timer} – For Flapping Links
 4. Split Horizon {I will not send update, from which interface I receive the update}
 5. Route poison or Poison reverse {Changing the metric & send}
- RIP = Hold down, Split horizon, Route Poison
- EIGRP = Split horizon, Poison Reverse
- OSPF = Link state protocols does not need loop prevention

EIGRP Lab- Concepts

0. Topology
1. Host Names {PT & Hosts}
2. IP address
3. Serial
4. Routing protocols
 1. EIGRP
 1. Start EIGRP protocol i.e. give Autonomous system no.
 2. In Router Config mode
 1. Network Command i.e. Add Interface to EIGRP
 2. No Auto Summarization
 3. Change Bandwidth of the link
 4. Equal & Un-Equal Load Balancing
 5. To Verify
 1. Show ip eigrp Neighbors
 2. Show ip eigrp topology
 3. Show ip Route {"D" = EIGRP}



EIGRP - Topology



EIGRP LAB - Commands

- To configure EIGRP:

- R1(config)# router eigrp 1 {+ R2 & R3}
 - Router{config-router}# network [directly connected network address i.e. "C" in the Routing table]
 - R1{config-router}# network 10.1.24.0
 - R1{config-router}# network 10.1.34.0
 - R1{config-router}# no auto-summary
 - R1{config-router}# exit

- To configure link bandwidth:

- R1(config)# interface serial 0/1/0
 - R1(config-if)# bandwidth 256

①

- To configure unequal Load Balancing:

- R1(config)# router eigrp 1
 - R1(config-router) # variance 2

②

- To verify:

- R1# show ip eigrp neighbors
 - R1# show ip eigrp topology
 - R1# show ip eigrp interface details
 - R1# show ip route





[Lab Details](#)

[Main Menu >>>](#)



Routing Technologies

IPv6 Addressing

Serial/Static

Lesson 25



kumar6009@gmail.com



@air.ds2

Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3 280

IPv6 Serial/Static Lab - Concepts

- Serial
 - 0. Topology
 - 1. Hosts {PT & Hosts}
 - 2. Activate IPv6 service
 - 3. IPv6 addresses
 - 4. Serial {Clock rate}
- Static
 - 1. Ipv6 Static Command
- OSPF – Single Area
 - 0. Topology
 - 1. Hosts {PT & Hosts}
 - 2. Activate IPv6 service
 - 3. IPv6 addresses
 - 4. Serial {Clock rate}
 - 5. OSPF Command
 - 1. Start OSPF
 - 2. Router-ID
 - 3. Interface
 - 1. OSPF process ID
 - 2. OSPF area config

IPv6 –Topology



IPv6 – Commands {Serial/Static}

- To enable IPv6:
 - R1 (config)# ip routing { for ipv4 }
 - R1 (config)# **ipv6 unicast-routing**
- To configure ipv6 address:
 - R1 (config)# int fa0/0
 - R1 (config- if)# **ipv6 address 2001:55::1/64**
 - R1 (config-if)# no shut
- To configure Static:
 - R1 (config)# ipv6 route 2001:56::/64 2001:210:10:1::2
 - R2 (config)# ipv6 route 2001:55::/64 2001:210:10:1::1
- To verify:
 - R1# Show ipv6 interface brief
 - R1# show ipv6 route
 - R1# ping 2001:56::1



[Lab Details](#)

[Main Menu >>>](#)



Routing Technologies

IPv6 Addressing

EIGRP

Lesson 25



kumar6009@gmail.com



@air.ds2

Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3 284

IPv6 Serial/Static Lab - Concepts

- EIGRP
 - 0. Topology
 - 1. Hosts {PT & Hosts}
 - 2. Activate IPv6 service
 - 3. IPv6 addresses
 - 4. Serial {Clock rate}
 - 5. EIGRP Command
 - 1. Start EIGRP
 - 2. Router-ID & No Shut
 - 3. Interface
 - 1. EIGRP ASN

IPv6 –Topology



IPv6 – Commands {EIGRP}

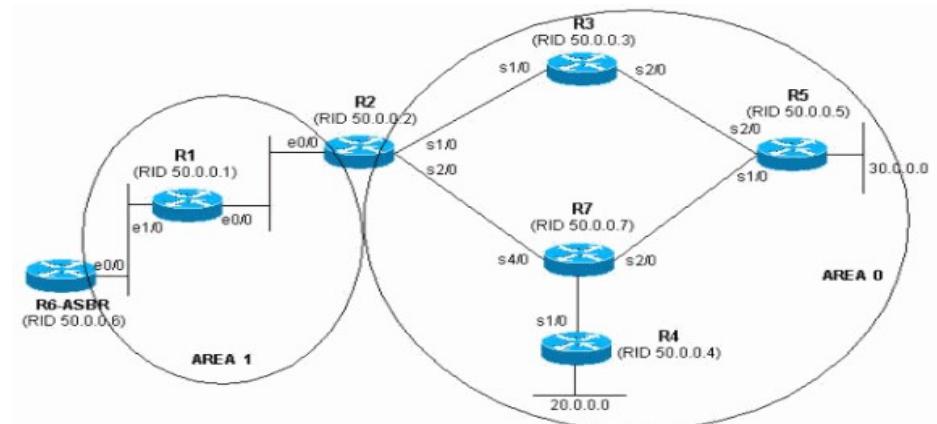
- To configure EIGRP: {Both R1 &R2}
 - R1(config)# ipv6 router eigrp 1
 - R1(config-router)# eigrp router-id 1.1.1.1
 - R1(config-router)# no shutdown
 - R1 (config-router)# exit
 - R1 (config)# int fa0/0
 - R1 (config-if)# ipv6 eigrp 1
 - R1 (config-if)# exit
 - R1 (config)# int S0/0/0
 - R1 (config-if)# ipv6 eigrp 1
 - R1 (config-if)# exit
- To Verify:
 - R2 # show IPv6 interface brief
 - R2 # show IPv6 protocols
 - R2 # show IPv6 route
 - R2 # ping 2001:55::1



IP Routing Technologies

OSPF Single Area

Lesson 17



OSPF Single Area - Concepts

- OSPF – Open Shortest path First
- Link State Routing Protocol i.e. routing by roadmap -Topology
- Updates - change of Link state only
- Classless routing protocol
- Interior Gateway Protocol
- Algorithm i.e. SPF{Shortest path first} or Dijkstra
- Metric = COST i.e. 100/Link bandwidth in Mbps
- Terminologies
 1. LSA i.e. Link State Advertisement
 2. Area {Summarization & Fault Containment}
 3. SPF i.e. Shortest Path First
 4. Router ID {Name of the Router in the OSPF process}
 5. Loopback interface & Address
 6. Backbone area – Area 0
 7. ABR i.e. Area Border Router
 8. ASBR i.e. Autonomous System Boundary Router
 9. DR i.e. Designated Router – Router, who gives topology details {i.e. MAP}
 10. BDR i.e. Backup DR
 11. Neighbor Database
 12. Link state Database {Topology}
 13. Routing Table {Best Routes}

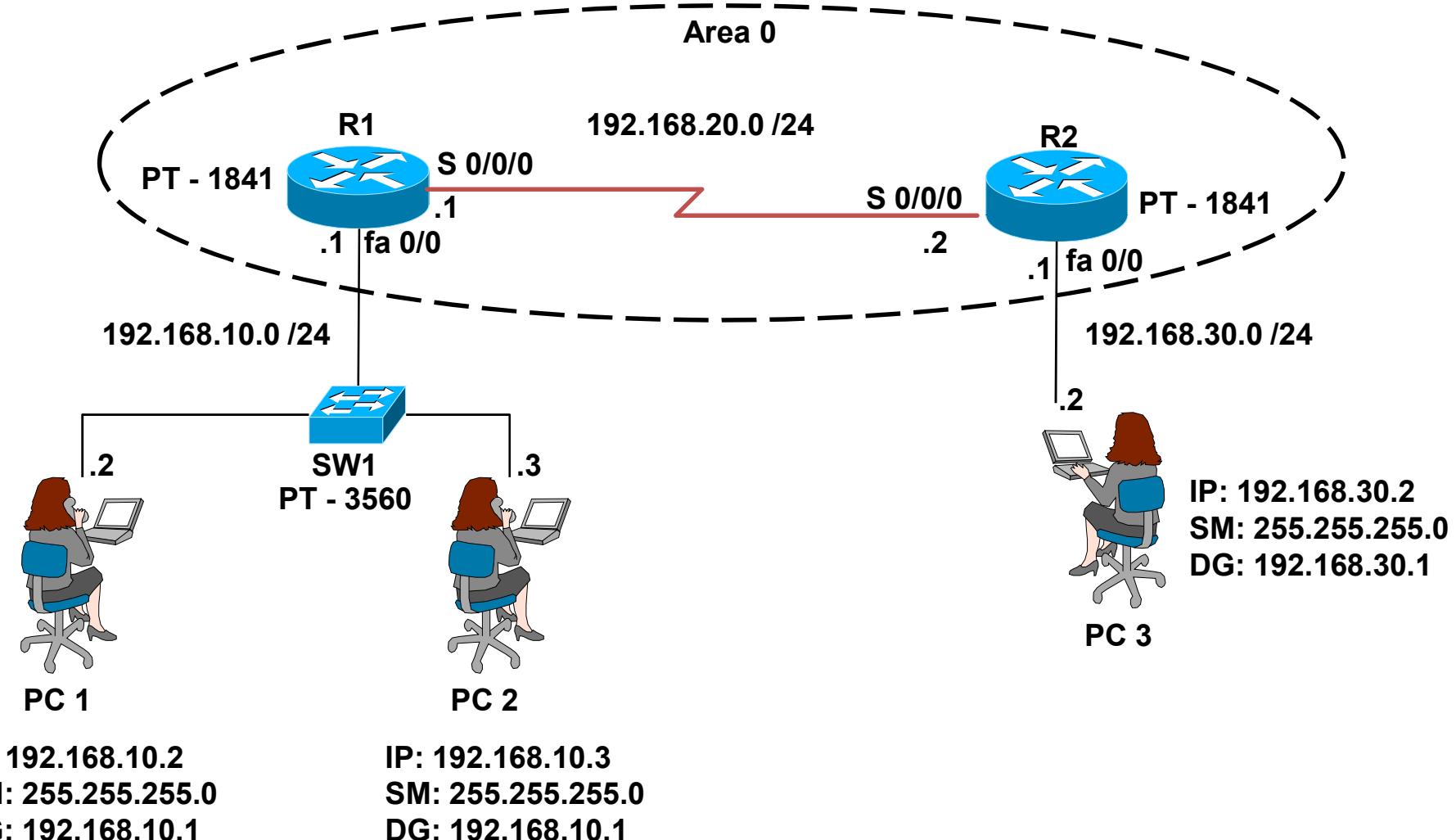


OSPF Single Area - Concepts

0. Topology
1. Host Names
2. IP address
3. Serial
4. Routing Protocol
 1. OSPF
 1. Start OSPF routing protocol
 1. Process ID
 2. Add Interfaces of directly connected Network Address by “NETWORK” command
 1. Wild card Mask
 2. Area Details
 3. Router –ID
 4. Passive Interface
 5. To verify
 1. Show IP route {"O" – ospf}
 2. Show ip ospf neighbors
 3. Show ip protocols
 4. Debug ip ospf events
 5. No debug all



OSPF Single Area - Topology



OSPF Single Area - Commands

- To configure OSPF:

R1:

- `R1(config)# router ospf 1 {+ R2}`

Syntax: Router(config-router)# network [directly connected network address] [wild card mask] area {no}

- `R1(config-router)# network 192.168.10.0 0.0.0.255 area 0`

- `R1(config-router)# network 192.168.20.0 0.0.0.255 area 0`

Process ID



- To configure ROUTER - ID

- `R1(config)# router ospf 1`

- `R1(config-router)# router-id 1.1.1.1`

- To configure passive interface:

- `R1(config)# router ospf 1`

- `R1(config-router)# passive interface default`

- `R1(config-router)# no passive interface serial 0/0/0`

- To verify:

- `R1# show ip route`

- `R1# show ip ospf neighbor`

- `R1# show ip protocols`

- `R1# debug ip ospf events`

- `R1# no debug all`

Wild Card Mask:

➤ Inverse to Subnet mask

➤ 0 = I care or match

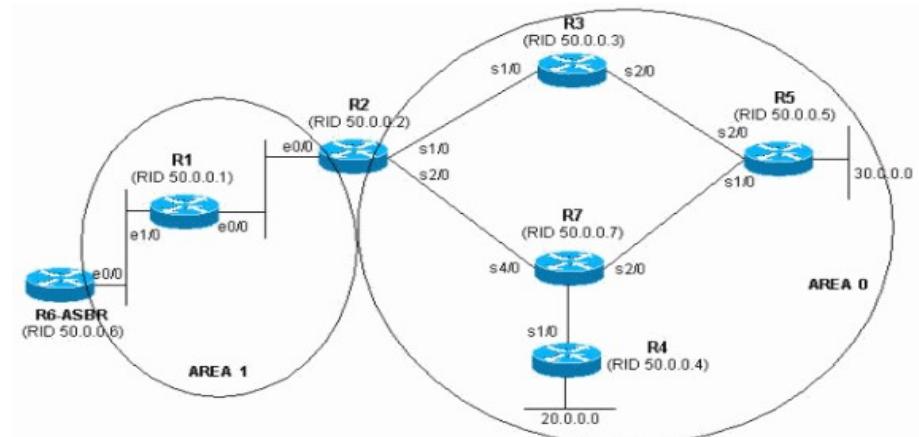
➤ 255 {1} = I don't care



Routing Technologies

OSPF Multi Area

Lesson 18



OSPF Multi Area- Concepts



1. Understanding OSPF neighbor Relationship

1. Determine your own Router-ID
2. Add interfaces to the Link state databases
3. Send a Hello message on chosen interfaces
4. Receive Hello
5. Check 4 parameters - Sent Reply Hello
6. Master – Slave Relationship Determined
7. DBD's are acknowledge and reviewed
8. Neighbors are synchronized

OSPF Multi Area- Concepts

Understanding OSPF neighbor Relationship:

1. Determine your own Router-ID
 1. Router's name in the ospf processes
 1. Highest active interface IP address
 2. Highest Loopback interface IP address
 3. Hard-coded using the "Router-ID" command
 2. Add interfaces to the Link state databases
 - Dictated by the network command
 3. Send a Hello message on chosen interfaces
 - Once every 10 seconds on Broadcast {Ethernet}/P-2-P networks
 - Once every 30 seconds on NBMA networks
 - NBMA – Non Broadcast Multi Access i.e. Frame Relay
 - Contains all sorts of information
 1. Router-ID
 2. Hello & Dead Timers *
 3. Network Mask *
 4. Area ID *
 5. Neighbors
 6. Router Priority
 7. DR/BDR IP address
 8. Authentication Password *



OSPF Multi Area- Concepts

Understanding OSPF neighbor Relationship:

4. Receive Hello

1. Check Hello/Dead Timers
2. Check network mask
3. Check Area ID
4. Check Authentication Passwords

5. Sent Reply Hello

- Am I listed as a neighbor in your hello packet
 - If yes, Reset Dead timer
 - If no, Add me as a new neighbor

6. Master – Slave Relationship Determined

- Determined by “priority# {Break tie} & Router ID
- Master sends Database Description {DBD} packet
 - DBD = Cliff notes of Link - State Database
- Slave sends its DBD packet



OSPF Multi Area- Concepts

Understanding OSPF neighbor Relationship:

7. DBD's are acknowledge and reviewed
 - Slave requests details {link state request – LSR}
 - Master sends updates {link state updates – LSU}
 - Master request details {LSR}
 - Slave sends updates {LSU}
8. Neighbors are synchronized
 - Full State
- States {OSPF State Finite Machine}
 1. Down – no Hello
 2. Attempt – send Hello
 3. Init = receive Hello
 4. 2way = DR & BDR
 5. Ex-start = M&S
 6. Ex-change = Send DBD
 7. Loading = LSU/LSR
 8. Full = Neighborhood process is DONE



OSPF Multi Area- Concepts

OSPF Metric:

- COST
 - 100/link Bandwidth – in – Mbps
- Common Costs:

Link Bandwidth	OSPF Cost
56 K	1785
64 K	1562
T1 {1.544}	64
E1 {2.048}	48
Ethernet {10 Mbps}	10
Fast Ethernet {100 Mbps}	1

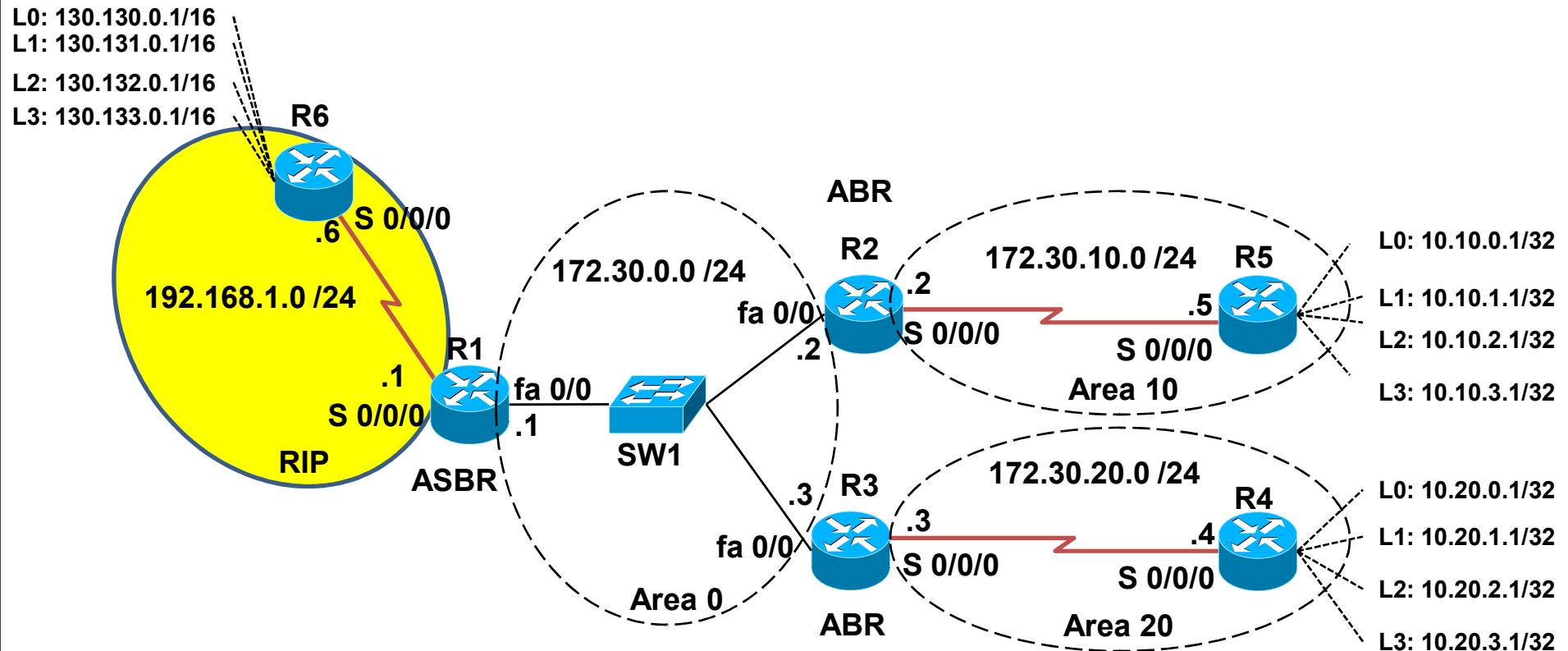


OSPF Multi Area Lab- Concepts

0. Topology
1. Host Names
2. IP address
3. Serial
4. Routing Protocol
 1. OSPF Single Area config – Area 0
 1. Network Address
 2. Wild card Mask
 3. Area Details
 2. OSPF Multi Area config – Area 10 & Area 20
 1. Network Address
 2. Wild card Mask
 3. Area Details
 3. OSPF Loopback interface & Address config
 4. OSPF Redistribution with RIP
5. To verify
 1. Show IP route {"O" – ospf, O IA – OSPF Inter Area, E2 –External Type }
 2. Show ip ospf neighbor
 3. Show ip protocols



OSPF Multi Area Lab - Topology



OSPF Multi Area Lab - Commands

- To configure OSPF:

R1:

- R1(config)# router ospf 1 {+ R2, R3, R4 & R5}

- *Syntax: Router(config-router)# network [directly connected network address] [wild card mask] area {no}*

- To configure loopback interface:

- R5(config)# interface loopback 0

- R5(config-if)# ip address 10.10.0.1 255.255.255.255

- To configure Redistribution:

- R1(config)# Router OSPF 1

- R1(config-router)# redistribute rip metric 99

- To verify:

- R1# show ip interface brief

- R1# show ip route

- R1# show ip ospf neighbor

- R1# show ip protocols

- R1# debug ip ospf events

- R1# no debug all





[Lab Details](#)

[Main Menu >>>](#)



Routing Technologies

IPv6 Addressing

OSPF

Lesson 25



kumar6009@gmail.com



@air.ds2

Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3 302

IPv6 Serial/Static Lab - Concepts

- OSPF – Single Area
 - 0. Topology
 - 1. Hosts {PT & Hosts}
 - 2. Activate IPv6 service
 - 3. IPv6 addresses
 - 4. Serial {Clock rate}
 - 5. OSPF Command
 - 1. Start OSPF
 - 2. Router-ID
 - 3. Interface
 - 1. OSPF process ID
 - 2. OSPF area config

IPv6 –Topology



IPv6 – Commands {OSPF}

- To configure OSPF: {Both R1 &R2}

- R1 (config)# ipv6 router ospf 1
 - R1 (config-router)# router-id 1.1.1.1
 - R1 (config-router)# exit
 - R1 (config)# int fa0/0
 - R1 (config-if)# ipv6 ospf 1 area 0
 - R1 (config-if)# exit
 - R1 (config)# int S0/0/0
 - R1 (config-if)# ipv6 ospf 1 area 0
 - R1 (config-if)# exit

- To Verify:

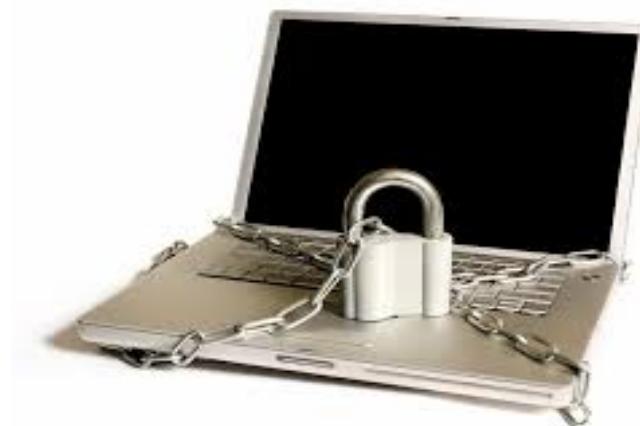
- R2 # show IPv6 interface brief
 - R2 # show IPv6 protocols
 - R2 # show IPv6 route
 - R2 # ping 2001:55::1



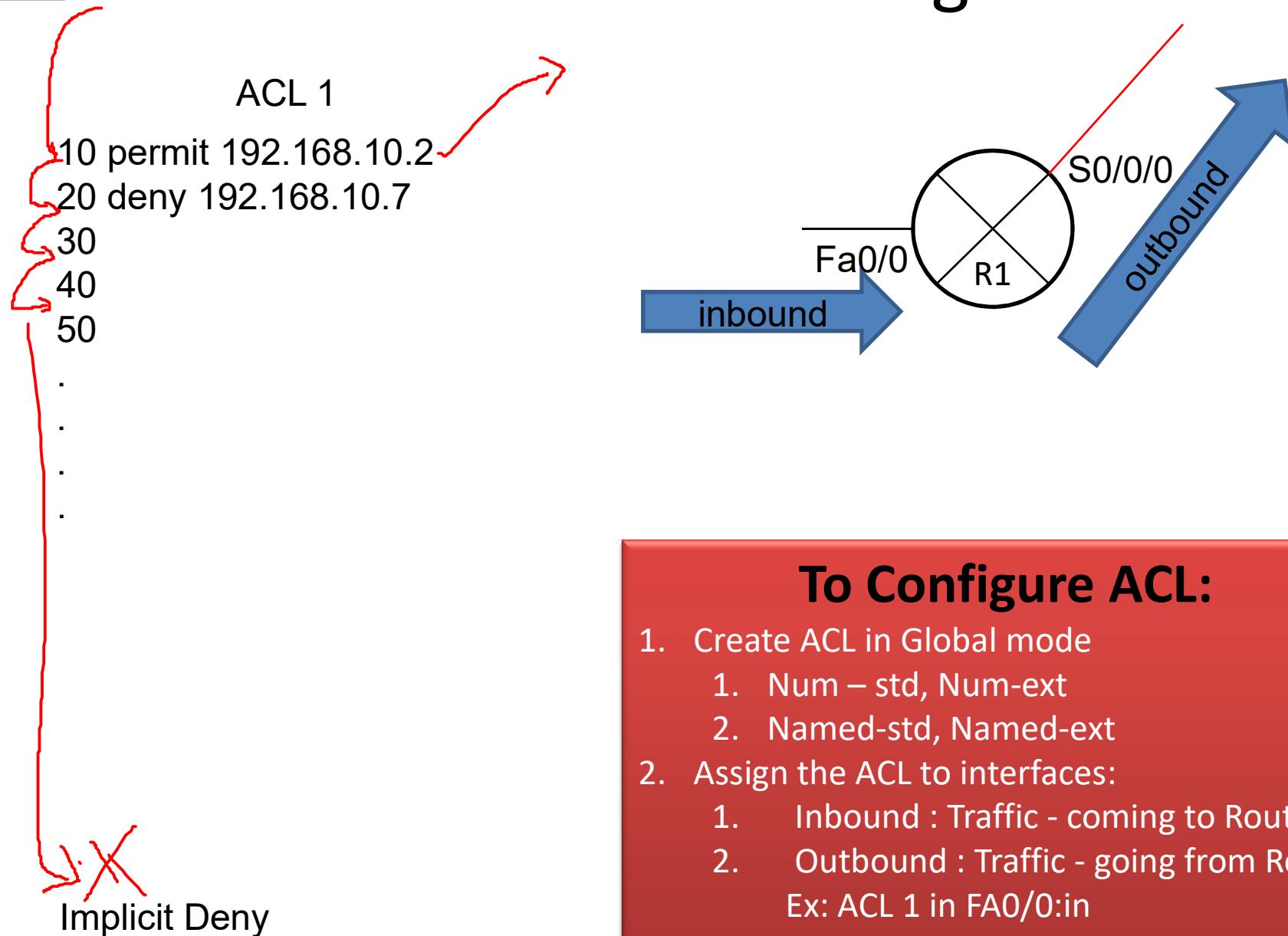
Infrastructure Security

ACL

Lesson 19



ACL – Terminologies

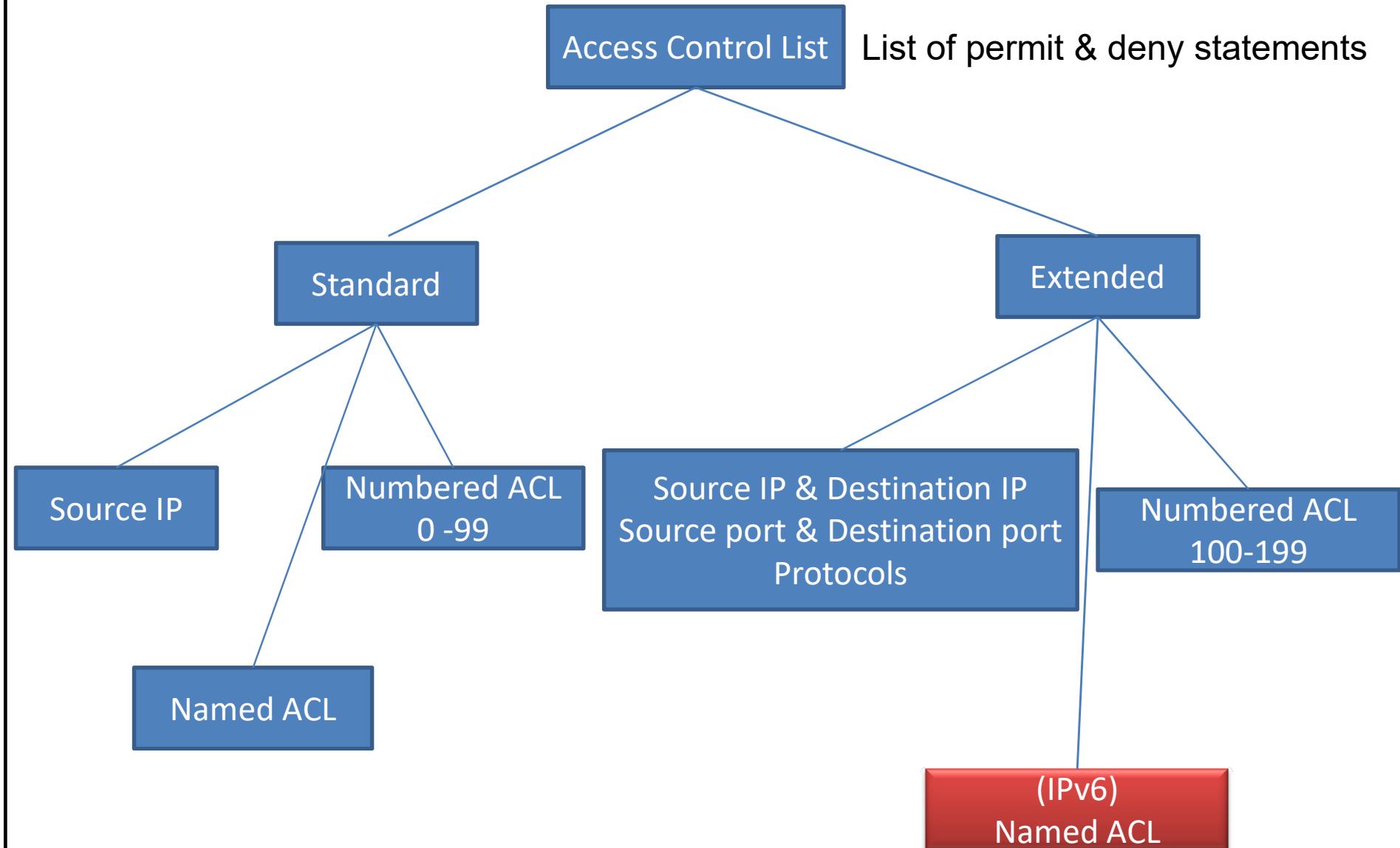


To Configure ACL:

1. Create ACL in Global mode
 1. Num – std, Num-ext
 2. Named-std, Named-ext
2. Assign the ACL to interfaces:
 1. Inbound : Traffic - coming to Router
 2. Outbound : Traffic - going from Router

Ex: ACL 1 in FA0/0:in

ACL – Terminologies



ACL – Terminologies

1. Access Control List
 - List of Permit & Deny statements
 - Implicit Deny
2. Types
 - Standard Access list
 - 1-99
 - Source IP address
 - Extended Access list
 - 100-199
 - Source ip address & destination ip address
 - Source Port & destination port
 - Protocol
3. Numbered Access list
4. Named Access list
5. Inbound : Traffic - coming to Router
6. Outbound : Traffic - going from Router

Infrastructure Security

IPv4 – Numbered -Standard ACL

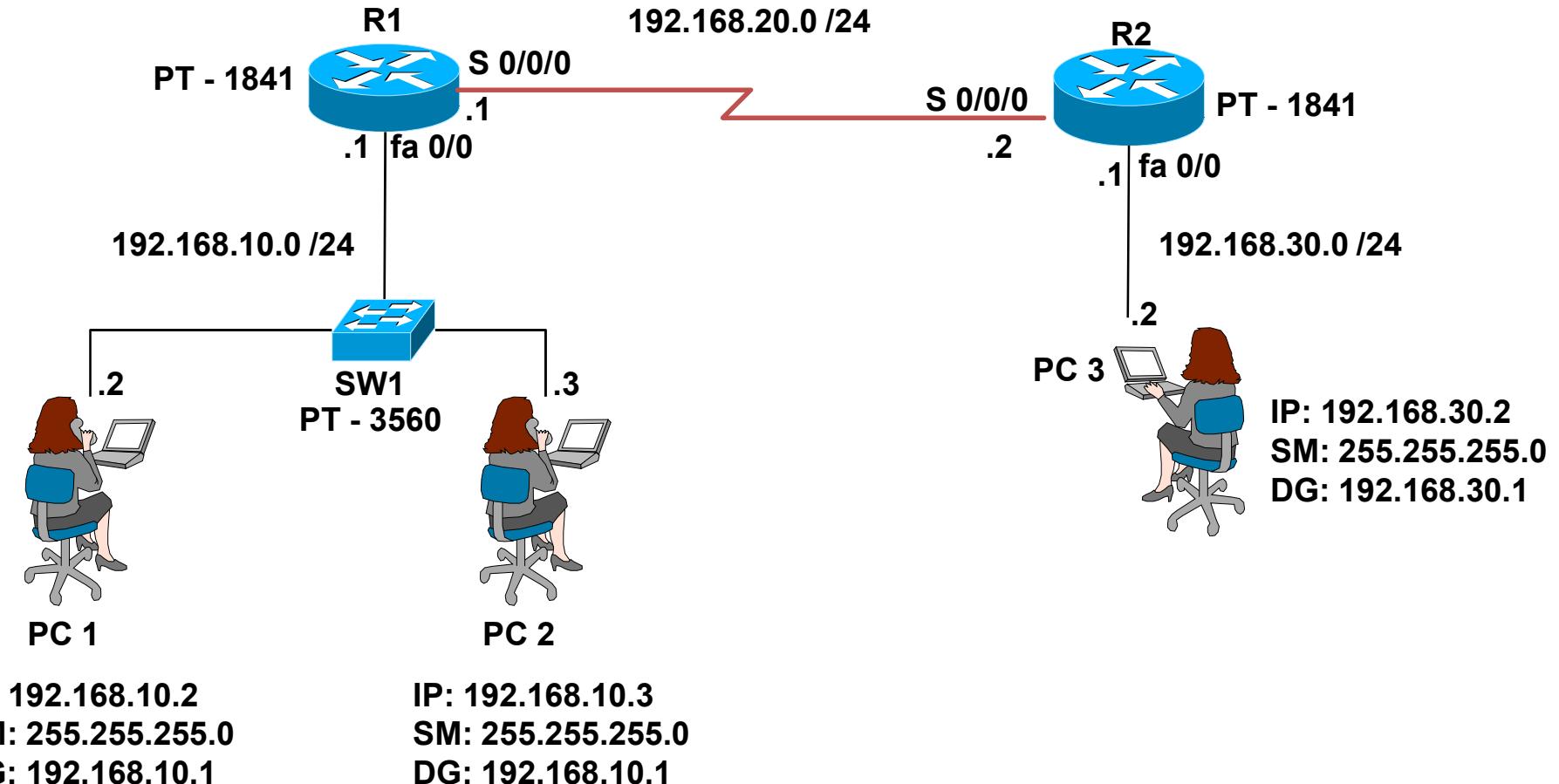
Lesson 19



ACL - LAB Concepts

0. Topology
1. Host Names
2. Ip address
3. Serial
4. Routing protocol
 1. RIP
5. Access list
 1. Permit PC1 i.e. IP = 192.168.10.2/24
6. Numbered Access list
 1. Standard access list
7. Ping
 1. PC1 -> PC3
 2. PC2 -> PC3

ACL - Topology



ACL - Commands

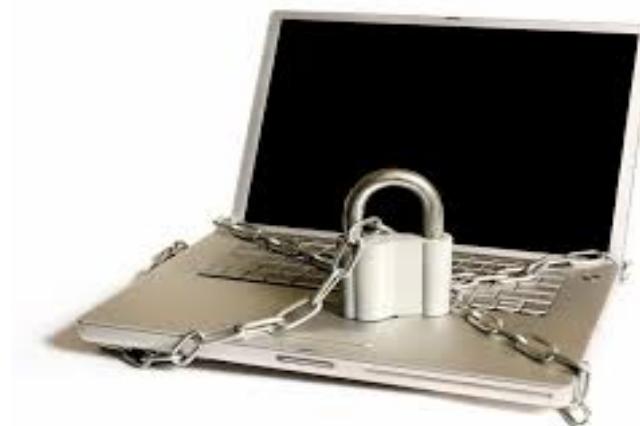
- To config standard Access-list:
 - R1(config)# access-list 1 permit 192.168.10.2
- To verify:
 - R1#show access-lists
- To config access list in the interface:
 - R1(config)# interface fast Ethernet 0/0
 - R1(config-if)# ip access-group 1 in
- To verify:
 - Ping
 - PC1 -> PC3
 - PC2 -> PC3



Infrastructure Security

ACL – IPv4 - Extended

Lesson 19



Extended ACLs



Extended ACLs can filter on:

- Source address
- Destination address
- Protocol
- Port numbers

Structure of an Extended IPv4 ACL



Extended ACLs (Cont.)

Using Port Numbers

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

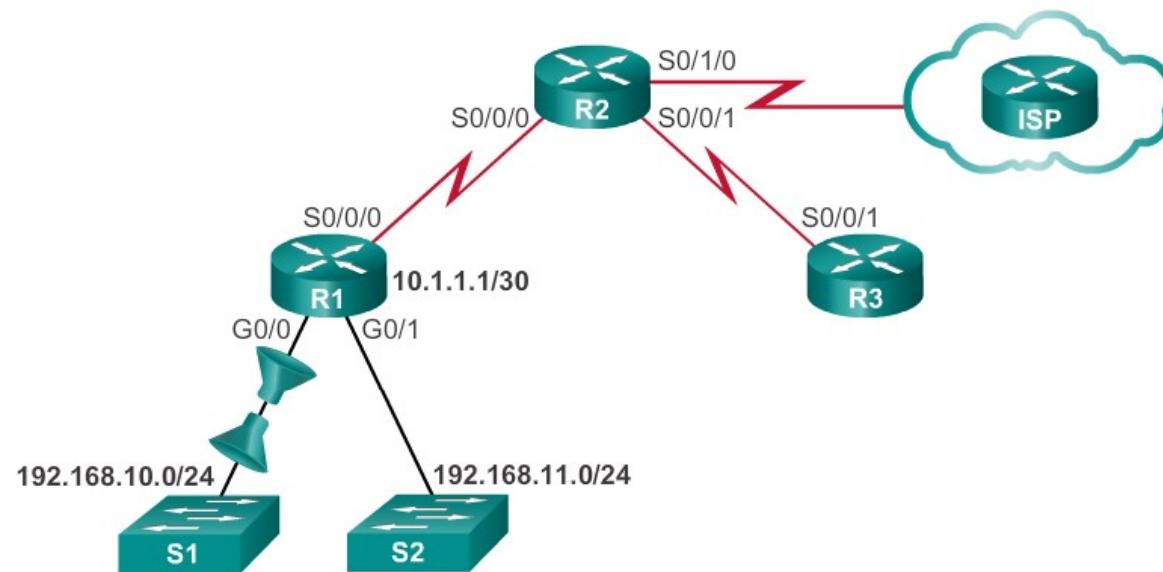
Using Keywords

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

Structure of an Extended IPv4 ACL



Applying Extended ACLs to Interfaces

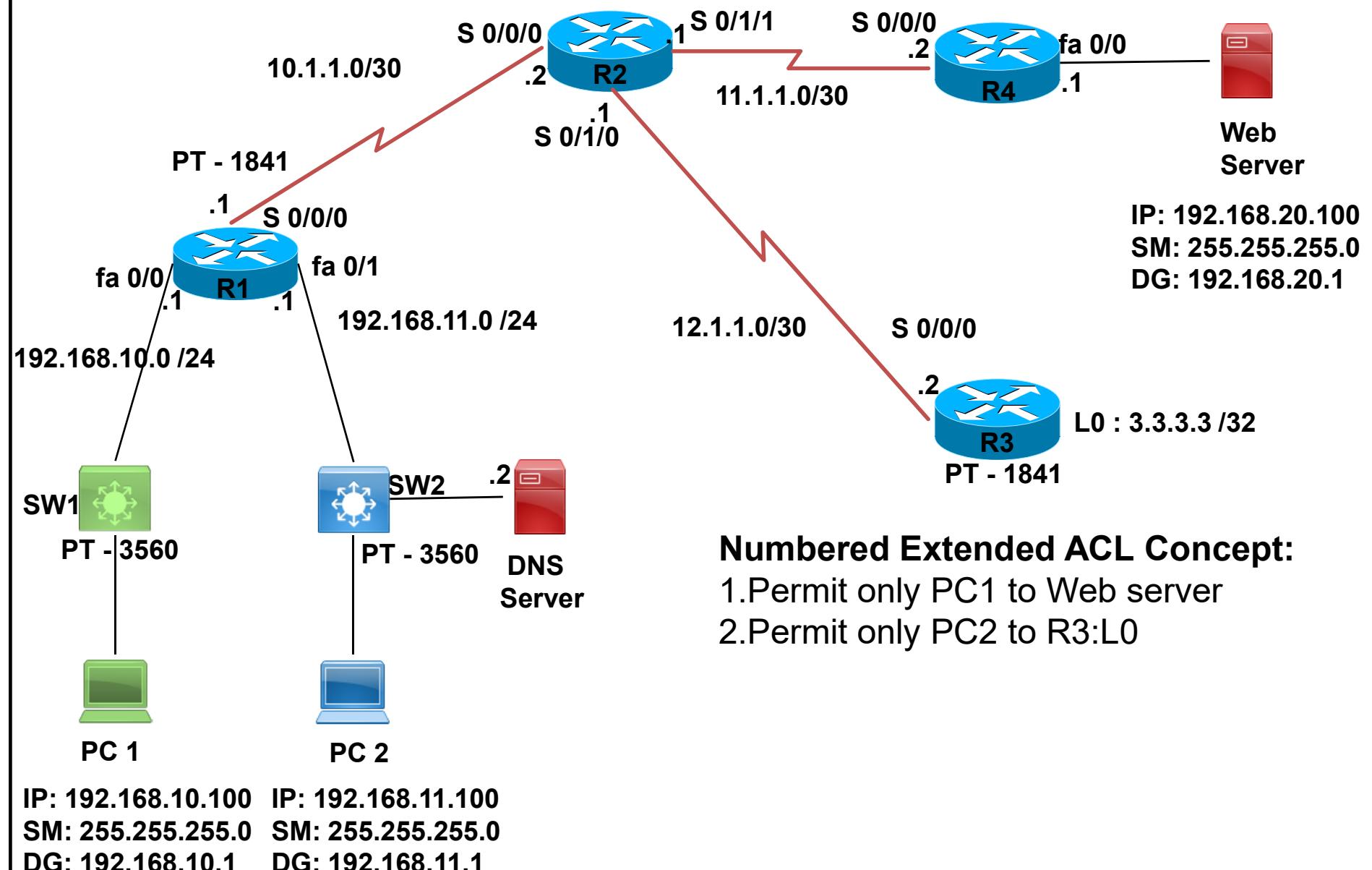


```
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)#access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)#interface g0/0
R1(config-if)#ip access-group 103 in
R1(config-if)#ip access-group 104 out
```

Configure Extended IPv4 ACLs



LAB -36 IPv4 Extended Numbered ACL



Numbered Extended ACL Concept:

1. Permit only PC1 to Web server
2. Permit only PC2 to R3:L0

IP: 192.168.10.100 IP: 192.168.11.100
 SM: 255.255.255.0 SM: 255.255.255.0
 DG: 192.168.10.1 DG: 192.168.11.1



kumar6009@gmail.com



@air.ds2

Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3

Infrastructure Security

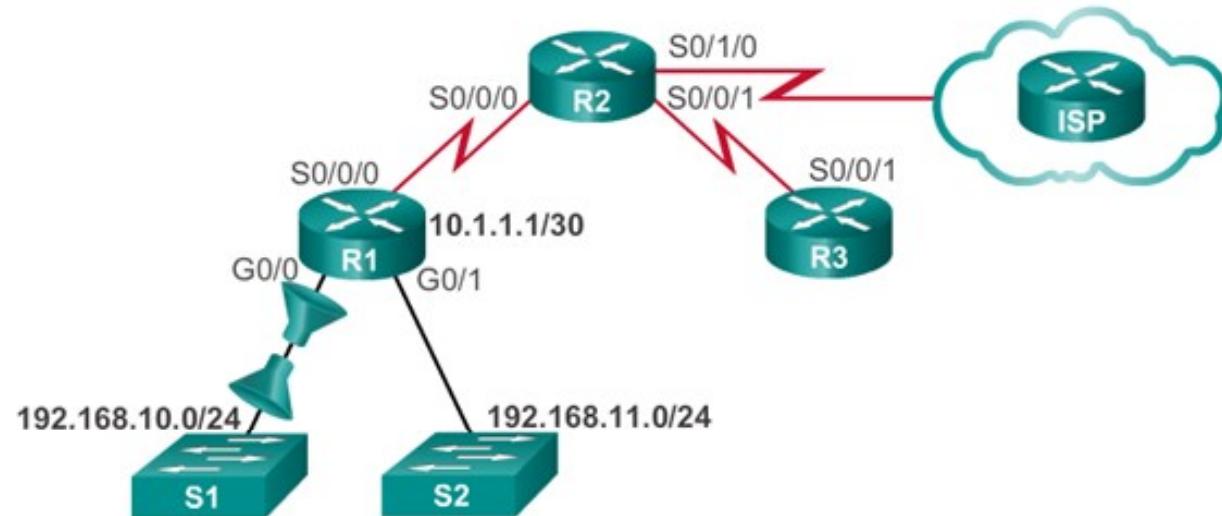
IPv4 – Named ACL

Lesson 19



Creating Named Extended ACLs

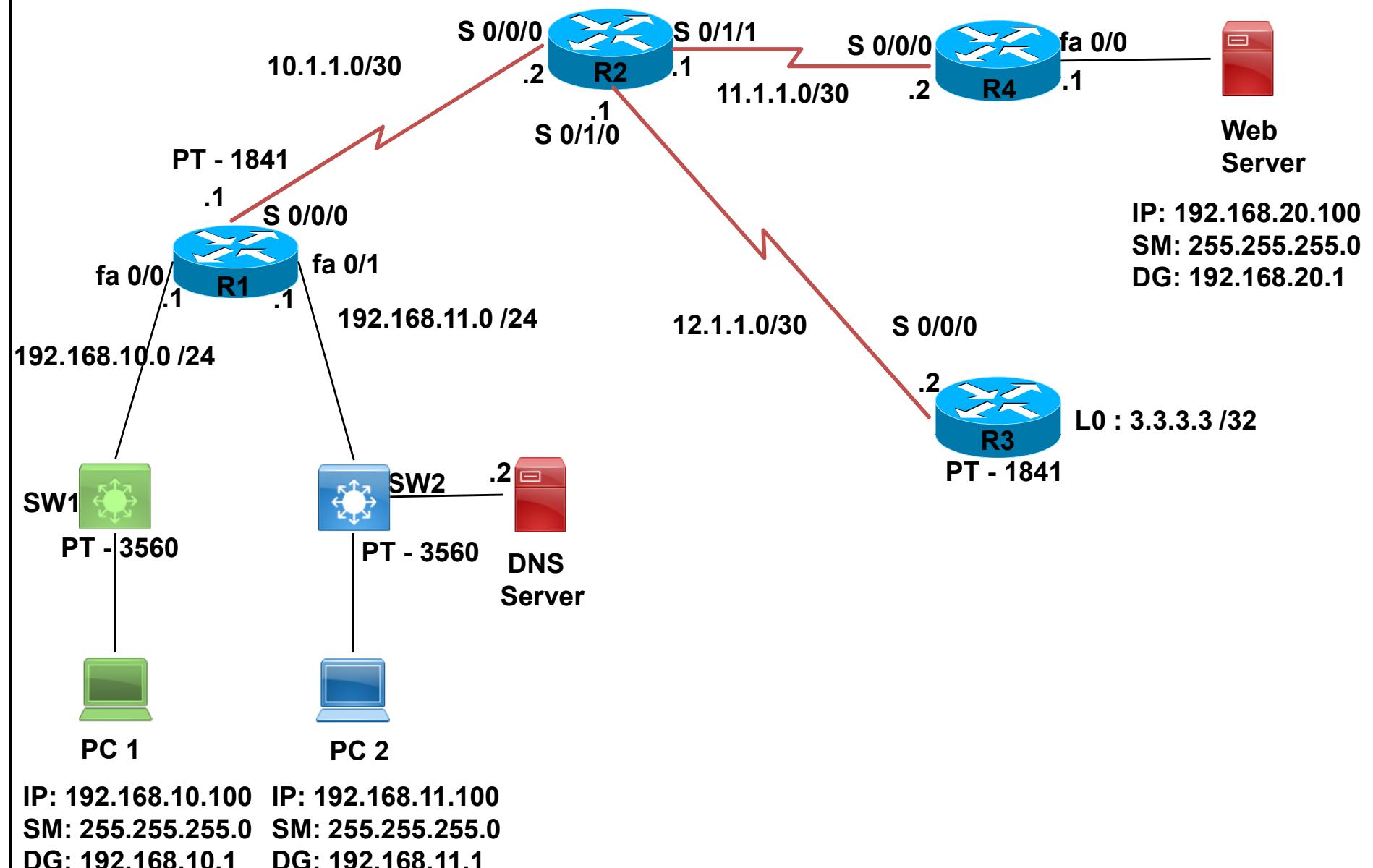
Creating Named Extended ACLs



```
R1(config)#ip access-list extended SURFING
R1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)#exit
R1(config)#ip access-list extended BROWSING
R1(config-ext-nacl)#permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)#exit
R1(config)#interface g0/0
R1(config-if)#ip access-group SURFING in
R1(config-if)#ip access-group BROWSING out
```



LAB -37 IPv4 Extended Named ACL



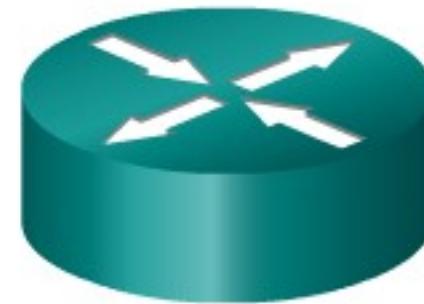
Infrastructure Security

ACL – IPv6 - Named

Lesson 19



Type of IPv6 ACLs



IPv4 ACLs

- Standard
 - Numbered
 - Named
- Extended
 - Numbered
 - Named

IPv6 ACLs

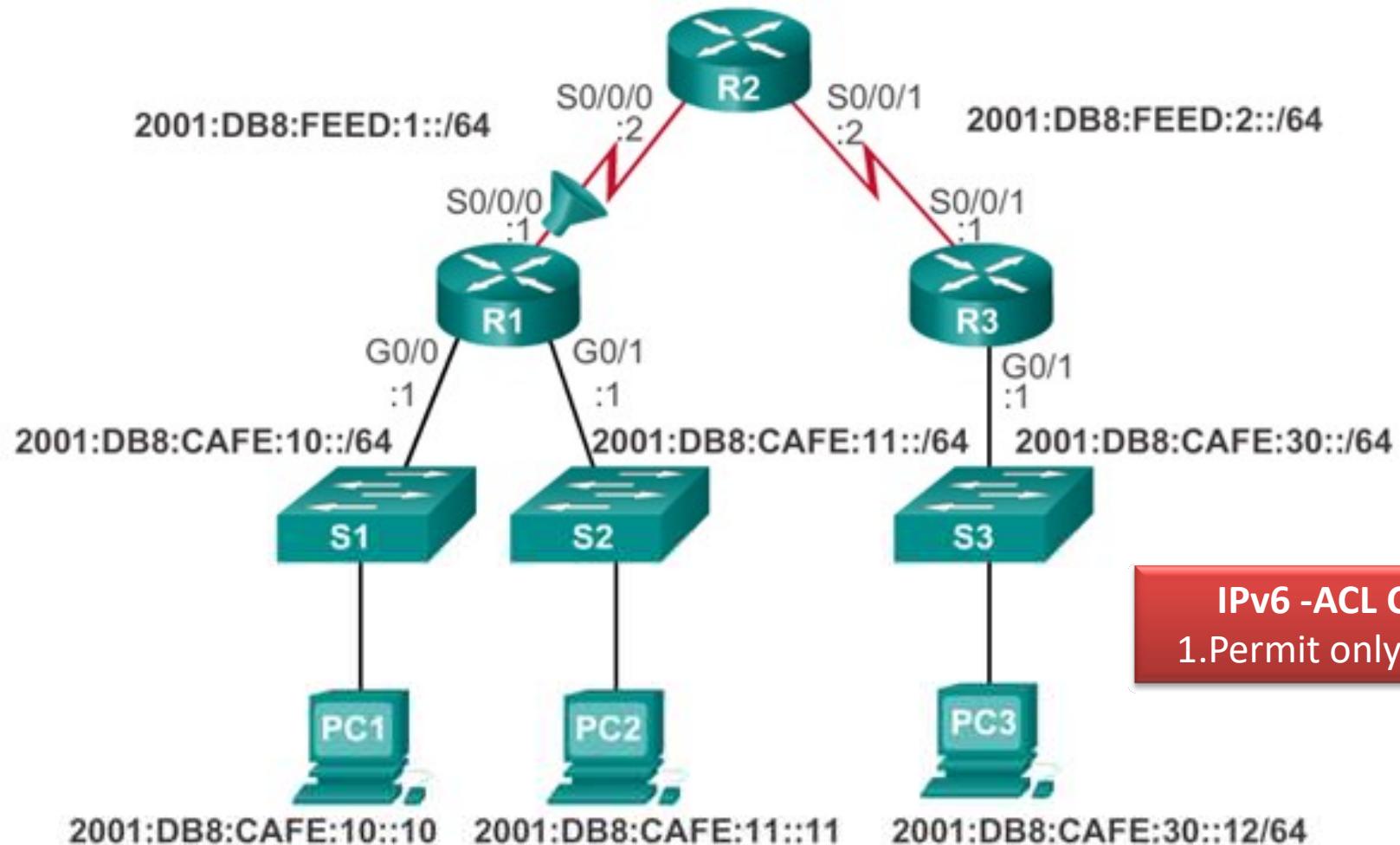
- Named only
- Similar in functionality to IPv4 Extended ACL

Comparing IPv4 and IPv6 ACLs

Although IPv4 and IPv6 ACLs are very similar, there are three significant differences between them.

- Applying an IPv6 ACL
 - IPv6 uses the **ipv6 traffic-filter** command to perform the same function for IPv6 interfaces.
- No Wildcard Masks
 - The prefix-length is used to indicate how much of an IPv6 source or destination address should be matched.
- Additional Default Statements
 - permit icmp any any nd-na**
 - permit icmp any any nd-ns**

Applying an IPv6 ACL to an Interface



```
R1(config)#interface s0/0/0
R1(config-if)#ipv6 traffic-filter NO-R3-LAN-ACCESS in
```

Infrastructure Services

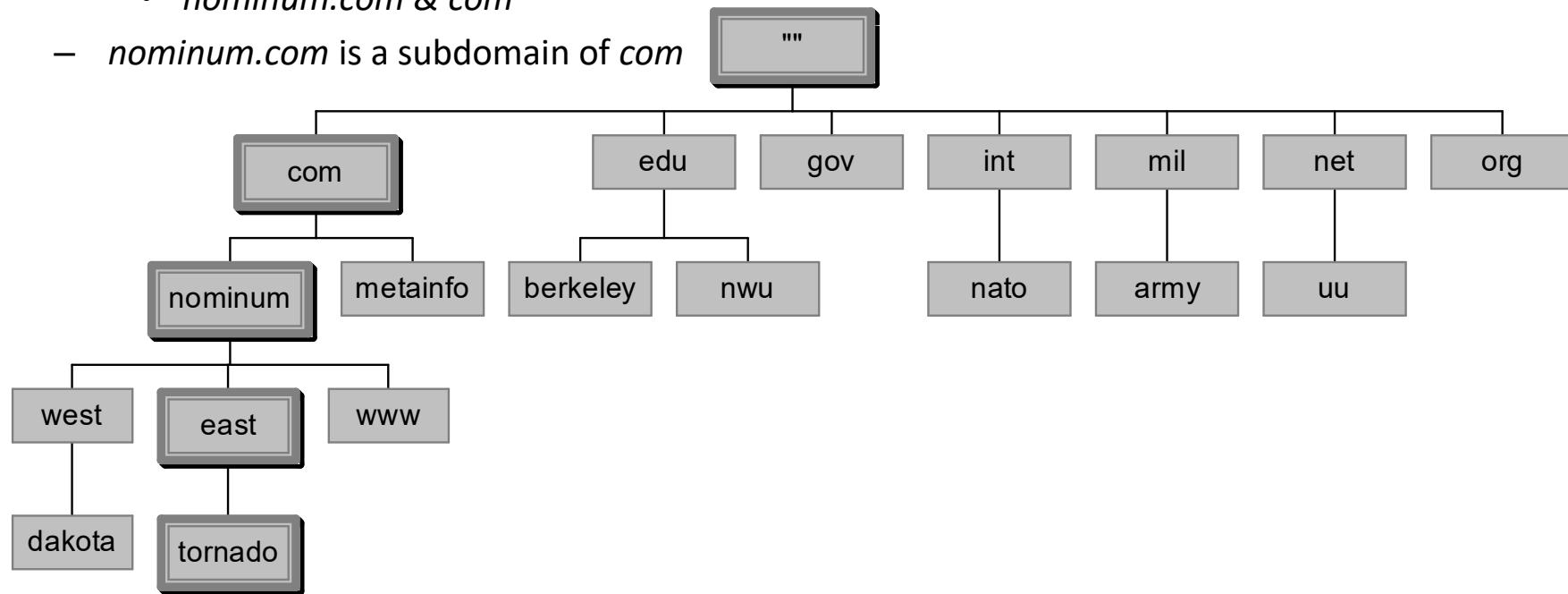
DNS

Lesson 33



DNS- Domain Name Service

- A *domain name* is the sequence of labels from a node to the root, separated by dots ("."s), read left to right
 - The name space has a maximum depth of 127 levels
 - Domain names are limited to 255 characters in length
- A node's domain name identifies its position in the name space
- One domain is a subdomain of another if its domain name ends in the other's domain name
 - So *sales.nominum.com* is a subdomain of
 - *nominum.com* & *com*
 - *nominum.com* is a subdomain of *com*



Infrastructure Services

DHCP

Lesson 33



DHCP

Dynamic Host Configuration Protocol:

- Dynamic - Automatically
- Host - PC, Router, Switch...
- Configuration
 - » IP address,
 - » Subnet Mask
 - » Default Gateway
 - » DNS server address
 - » Domain name
 - » Leased period(24 Hrs)
- Protocol - set of rules i.e. do's & don'ts

DHCP



```
Router(config)# hostname R1
```

```
R1(config)# ip dhcp excluded-address 10.10.0.1 10.10.0.20
```

```
R1(config)# ip dhcp pool dpool1
```

```
R1(dhcp-config)# import all {to activate}
```

```
R1(dhcp-config)# network 10.10.0.0 255.255.255.0
```

```
R1(dhcp-config)# default-router 10.10.10.10
```

```
R1(dhcp-config)# dns-server 192.168.35.2
```

```
R1(dhcp-config)# domain-name Hublic.com
```

```
R1(dhcp-config)# exit
```

```
R1(config)# ip domain-name bsnl.com
```

```
R1(config)# ip name-server 192.168.11.12
```

To Verify:

```
R1# Show ip dhcp pool
```

```
R1# Show ip interface brief
```



Infrastructure Services

FHRP

Lesson 34



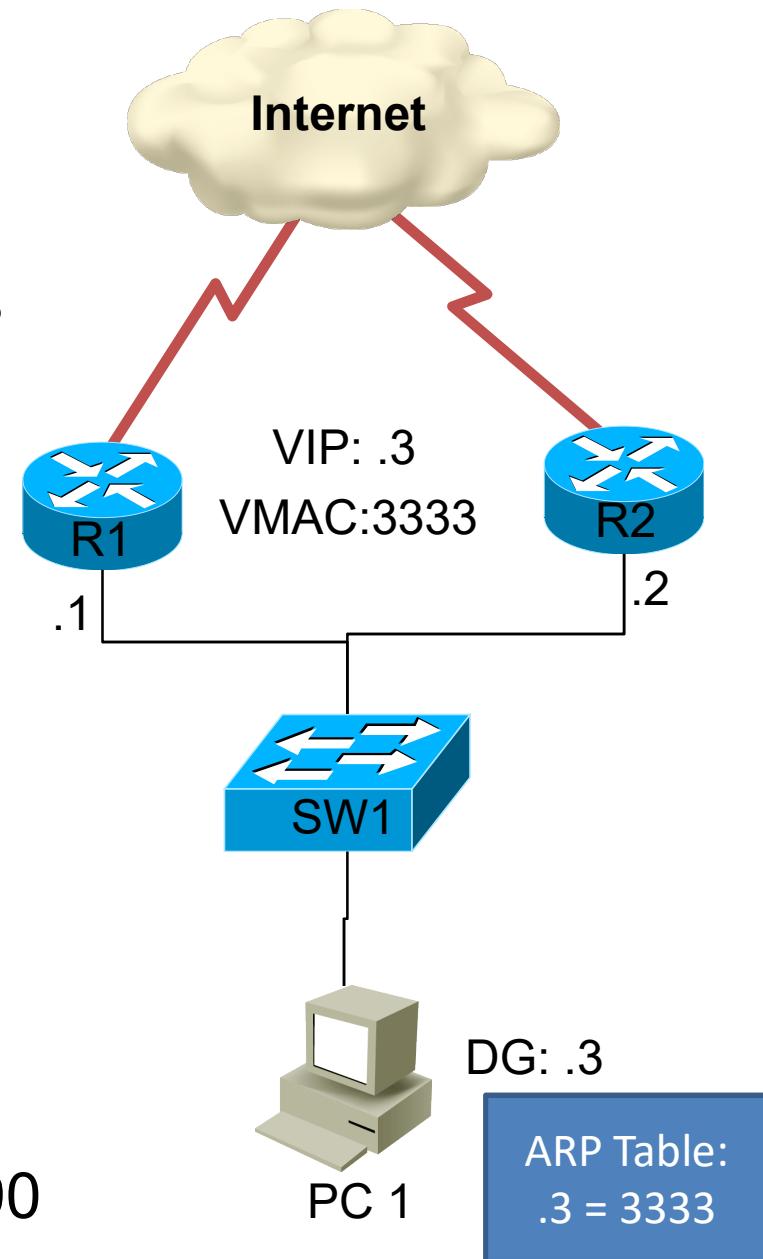
First Hop Redundancy Protocols{FHRP}

- Redundancy = Good
 - L2 = Spanning Tree Protocol
 - L3 = FHRP
- HSRP, VRRP, GLBP.... What is the difference?
- A focus on HSRP/VRRP & GLBP

Redundancy is Good:

Problems & Solution

- Problem 1:
 - How to switch Default gateway?
 - Solution: Virtual IP
- Problem 2 :
 - ARP Table – Cache [5 mins]
 - > solution : Virtual MAC
- Problem 3:
 - What If WAN link Fails?
 - > Solution : Interface Tracking
 - Intf down:>Priority 100 to 90

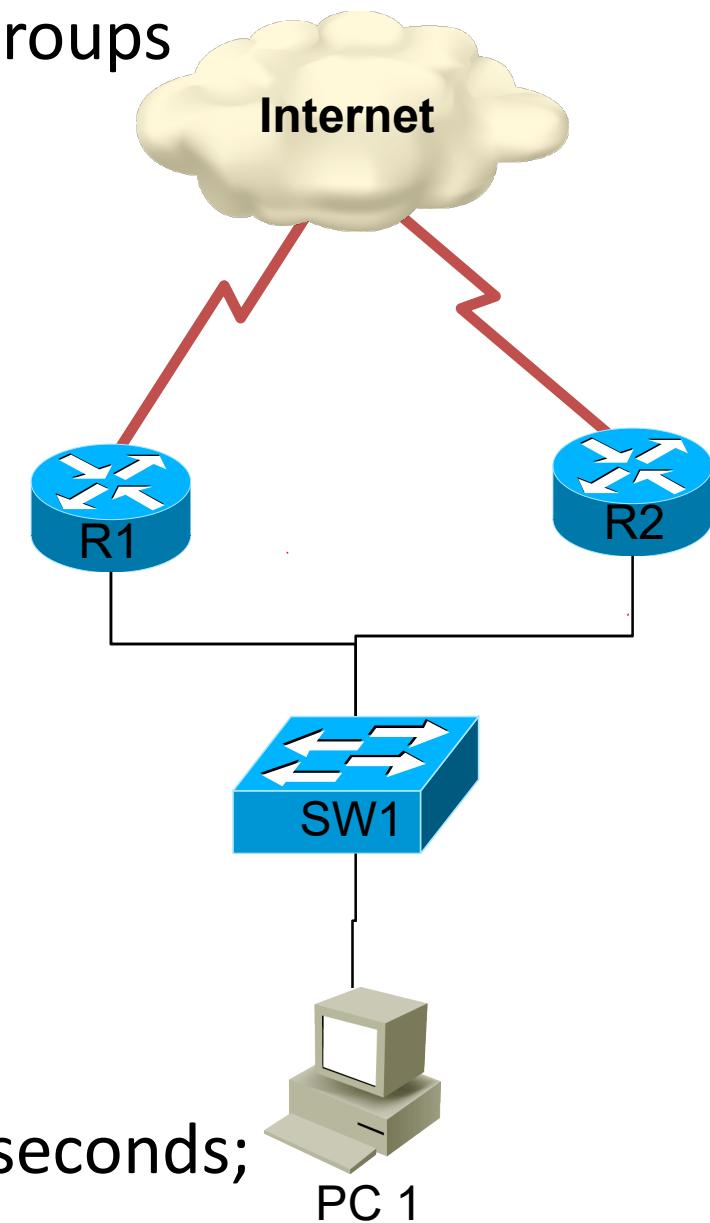


Flavors of L3 Redundancy {FHRP}

- Cisco Hot-Standby Router Protocol {HSRP}
 - Created by Cisco, for Cisco in 1994
 - Hello = 3 seconds; Hold = 10 seconds
- Virtual Router Redundancy Protocol {VRRP}
 - Created by IETF in 1999 (open standard)
 - Hello = 1 second; Hold = 3 seconds
 - We can configure existing Router interface IP address as virtual IP address
- Gateway(Router) Load Balancing Protocol {GLBP}
 - Created by Cisco, for Cisco in 2005
 - Hello = 3 seconds; Hold = 10 seconds
 - Identical to HSRP
 - But allow Active(50%)-Active(50%) Load-Balancing

A Focus on HSRP/VRRP

- Gateways organized into standby groups
- One gateway Active, others in standby state
- Phantom {Virtual} router ip address need to configured
 - MAC address generated
 - HSRP Range:
 - V1 : 0000.0c07.ACxx
 - V2 : 0000.0C9F.F000 to 0000.0C9F.FFFF
- Hello messages sent once every 3 seconds; Dead after 10 seconds



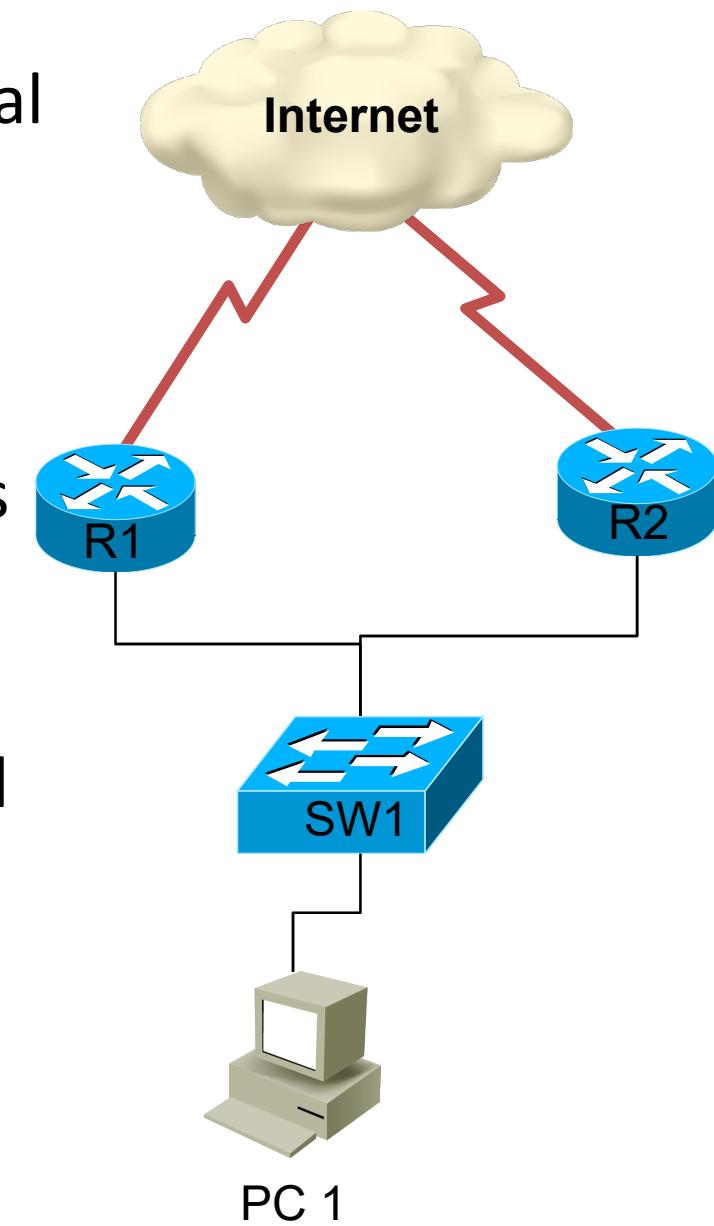
A Focus on GLBP

- One Gateway assigned Active Virtual Gateway {AVG} role
- Additional gateways act as a Active Virtual Forwarders {AVF}
- Phantom {Virtual} router ip address need to configured
 - MAC address generated
- AVG responds to ARP request, Load balances by different MAC replies
- Hello messages sent once every 3 seconds; Dead after 10 seconds

AVG – Response to ARP Requests

R1's MAC 1 - 1111:1111:1111

R2's MAC 2 – 2222:2222:2222:



IP Services

HSRP

Lesson 35



HSRP Base Configuration – Lab24

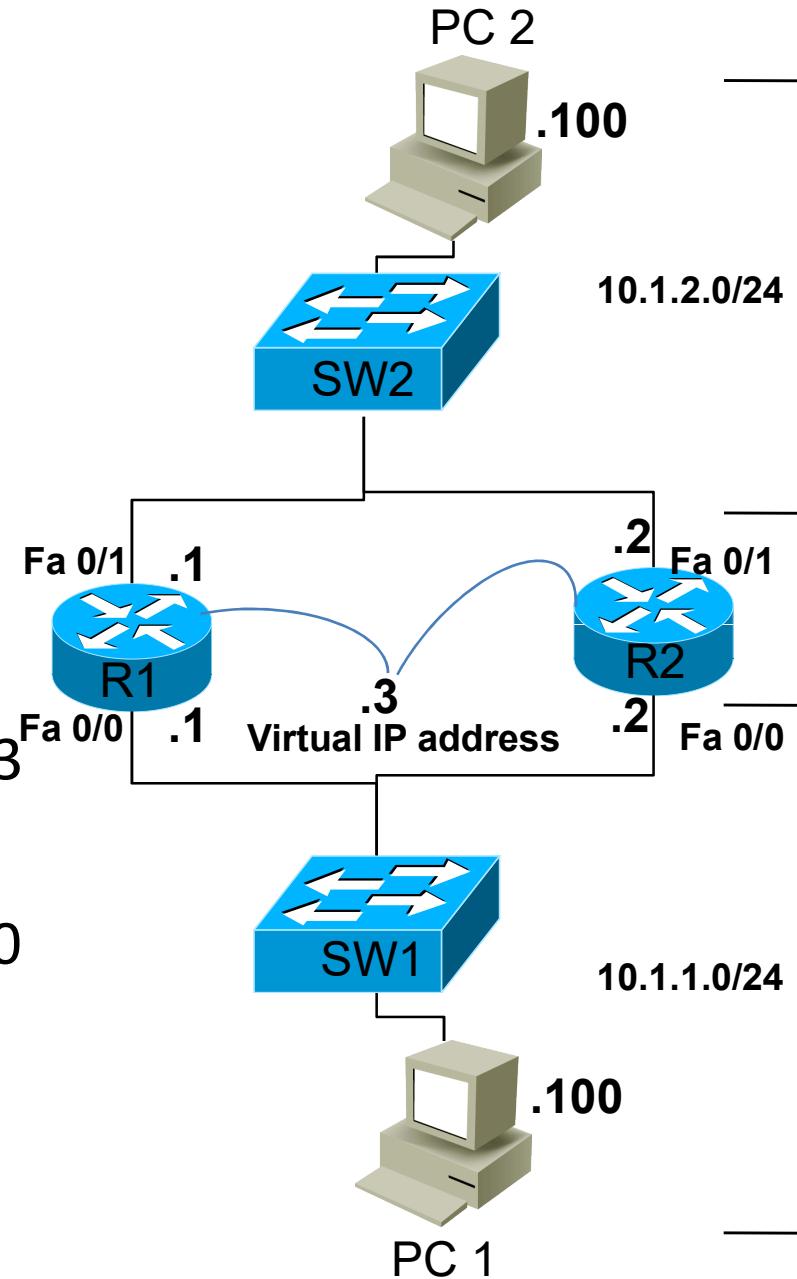
- Step 1 : Create Standby Group
- Step 2 : Assign virtual IP address
- Step 3 : Verify
- Step 4 : Optimize and Tune

Commands:

- R1# Show IP int brief {+ R2}
- R1{config }# Interface fa0/0
- R1{config-If}# standby 1 ip 10.1.1.3
- R1{config-If}# standby 1 preempt
- R1{config-If}# standby 1 priority 90

To verify:

- R1# show arp
- R1# show standby brief



IP Services

NAT – Static

Lesson 21

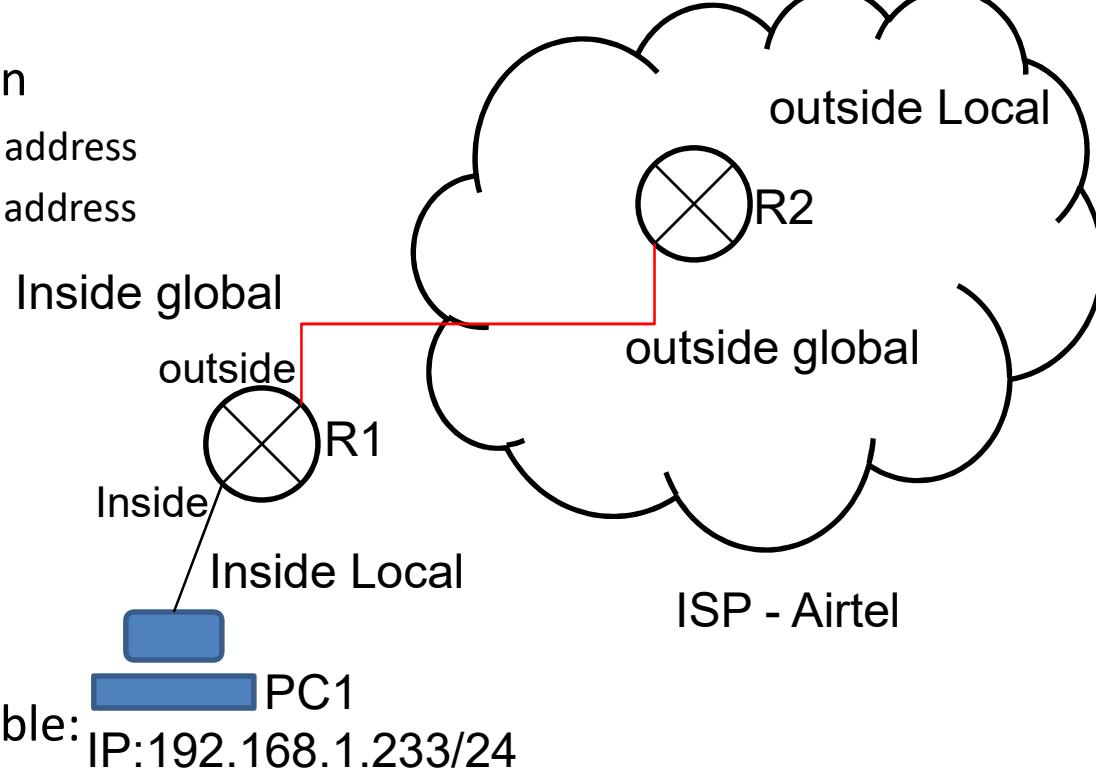


Network Address Translation

- Network Address Translation
 - Private ip address -> Public Ip address
 - Public ip address -> Private ip address
- NAT Terminologies
 - Inside
 - Outside
 - Inside Local Address
 - Inside Global Address
 - Outside Global Address
 - Outside Local Address
- Private IP Address Range Table:

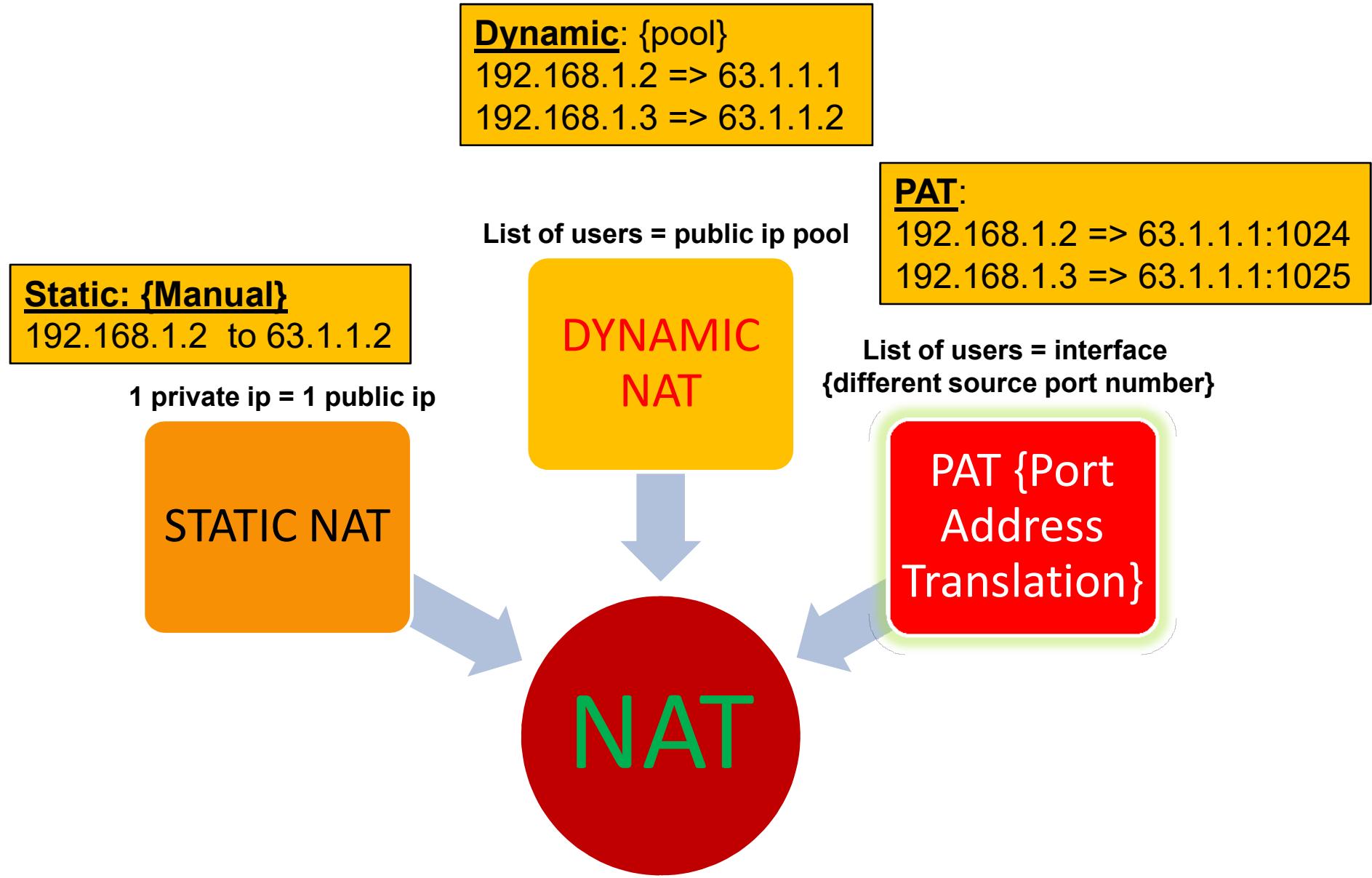
Class	Start IP Address	End IP Address
Class A {1-126}	10.0.0.0	10.255.255.255
Class B {128-191}	172.16.0.0	172.31.255.255
Class C {192-223}	192.168.0.0	192.168.255.255

IP:192.168.1.233/24



Class	Start IP Address	End IP Address
Class A {1-126}	10.0.0.0	10.255.255.255
Class B {128-191}	172.16.0.0	172.31.255.255
Class C {192-223}	192.168.0.0	192.168.255.255

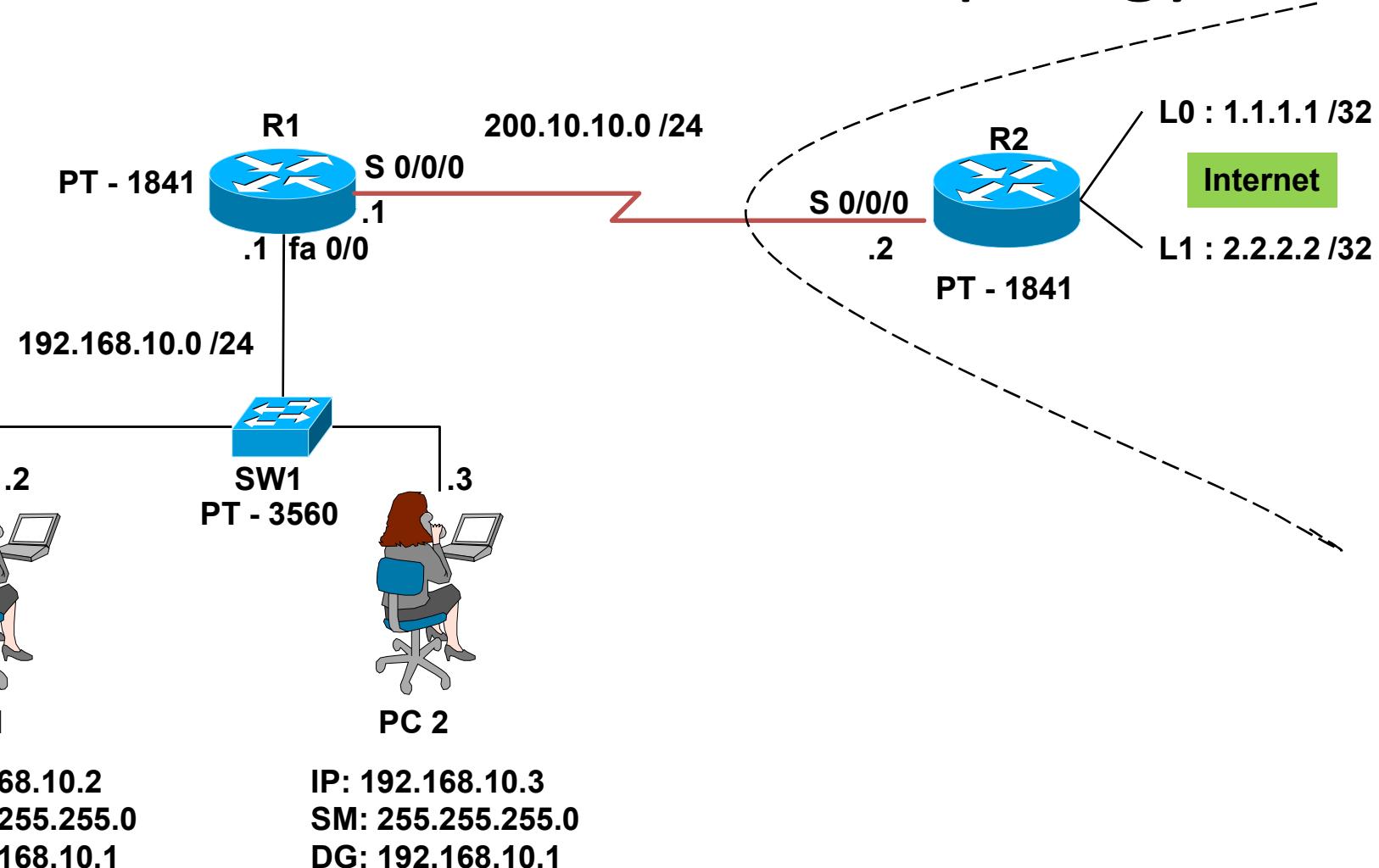
Network Address Translation



NAT – Static - LAB Concepts

0. Topology
1. Host Names
2. Ip address
3. Serial
4. Routing protocol
 1. RIP
5. R1: NAT
 1. Static
 1. Inside/Outside
 2. Static NAT command

NAT-Static/Pool/PAT- Topology



NAT- Static- Commands

- To config inside/outside:
 - R1# configure terminal
 - R1(config)# Interface Fast Ethernet 0/0
 - R1(config-if)# ip nat inside
 - R1(config-if)# exit
 - R1# configure terminal
 - R1(config)# Interface serial 0/0/0
 - R1(config-if)# ip nat outside
 - R1(config-if)# exit
- To configure Static NAT:
 - R1(config)# ip nat inside source static 192.168.10.2 200.10.10.3
- To verify
 - Ping
 - PC1 -> L0
 - R1# show ip nat translations

IP Services

NAT – Dynamic

Lesson 22

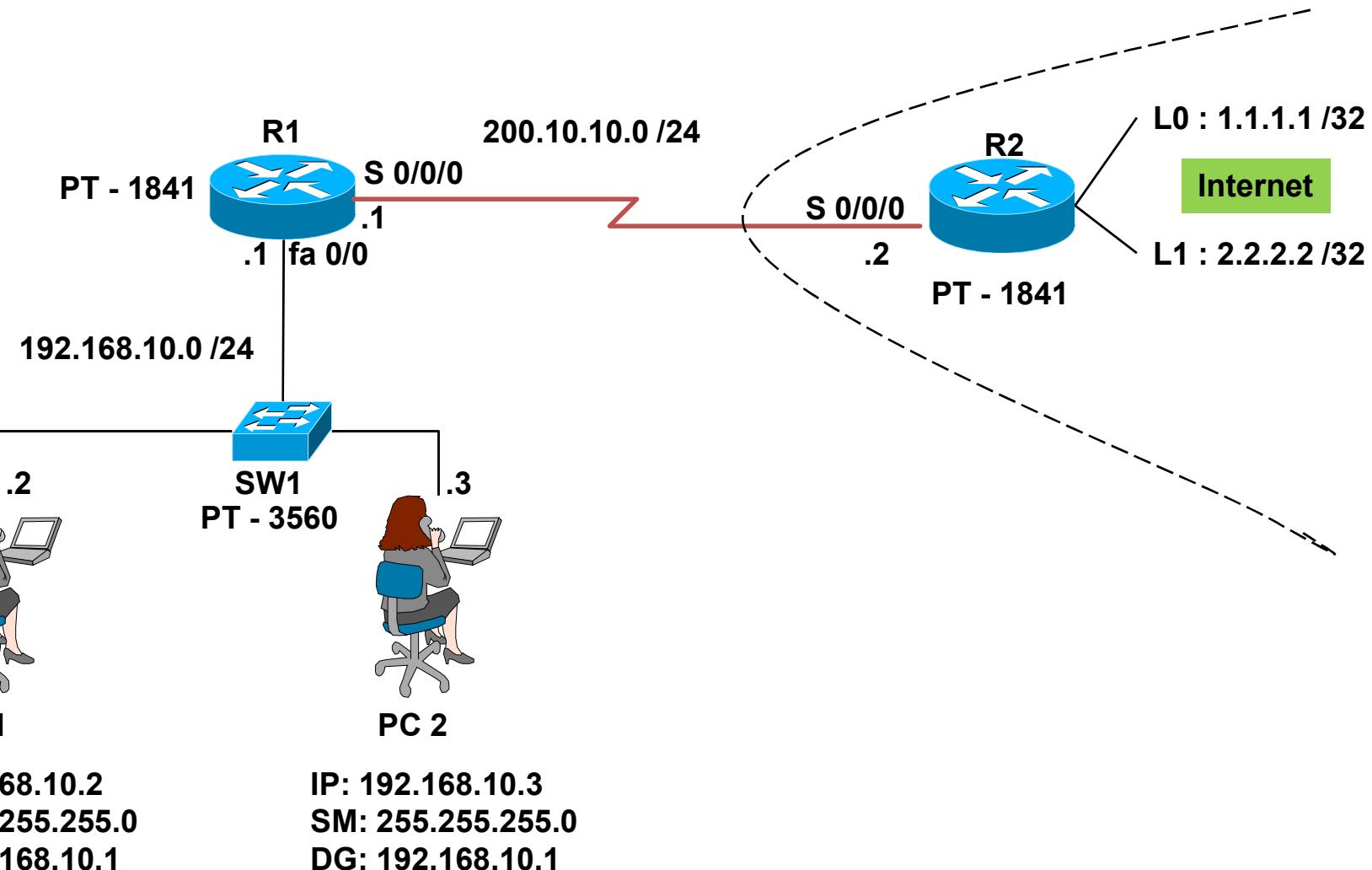


NAT-Dynamic - LAB Concepts

0. Topology
1. Host Names
2. Ip address
3. Serial
4. Routing protocol
 1. RIP
5. NAT
 1. Dynamic
 1. Inside/Outside
 2. Create public ip address pool
 3. Create list for users
 4. Dynamic NAT command



NAT-Dynamic- Topology



NAT- Dynamic - Commands

- To config inside/outside:
 - R1# configure terminal
 - R1(config)# Interface Fast Ethernet 0/0
 - R1(config-if)# ip nat inside
 - R1(config-if)# exit
 - R1(config)# Interface serial 0/0/0
 - R1(config-if)# ip nat outside
 - R1(config-if)# exit
- To configure NAT Public IP Pool:
 - R1(config)# ip nat pool npool 200.10.10.3 200.10.10.6 netmask 255.255.255.0
- To configure list of users:
 - R1(config)# ip access-list standard 1
 - R1(config-std-nacl)# permit 192.168.10.0 0.0.0.255
 - R1(config-std-nacl)# exit
- To configure Dynamic NAT:
 - R1(config)# ip nat inside source list 1 pool npool
- To verify:
 - Ping
 - PC1 -> L0
 - PC2 -> L1
 - R1# show ip nat translations



IP Services

NAT – PAT

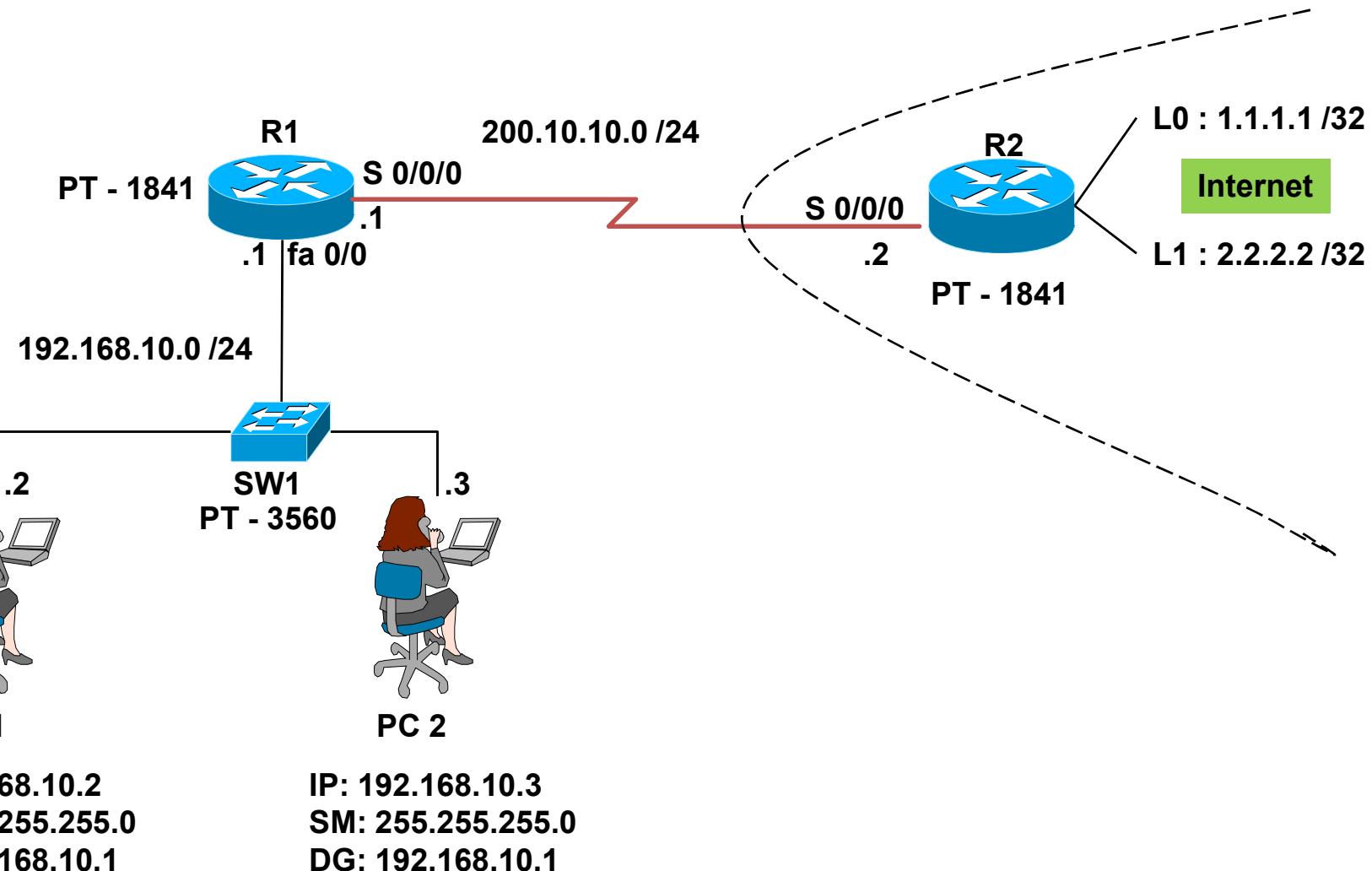
Lesson 23



NAT- PAT- LAB Concepts

0. Topology
1. Host Names
2. Ip address
3. Serial
4. Routing protocol
 1. RIP
5. PAT
 1. Inside/Outside
 2. Create list for users
 3. PAT command
6. Ping
 - PC1 -> L0
 - PC2 -> L1
5. To verify:
 - R1: # show nat translations

NAT- PAT- Topology



NAT- PAT- Commands

- To config inside/outside:
 - R1# configure terminal
 - R1(config)# Interface Fast Ethernet 0/0
 - R1(config-if)# ip nat inside
 - R1(config-if)# exit
 - R1# configure terminal
 - R1(config)# Interface serial 0/0/0
 - R1(config-if)# ip nat outside
 - R1(config-if)# exit
- To configure list of users & PAT command:
 - R1(config)# ip access-list standard 1
 - R1(config-std-nacl)# permit 192.168.10.0 0.0.0.255
 - R1(config-std-nacl)# exit
 - R1(config)# ip nat inside source list 1 interface serial 0/0/0 overload
- To verify
 - Ping
 - PC1 -> L0
 - PC2 -> L1
 - R1# show ip nat translations

IP Services

NTP

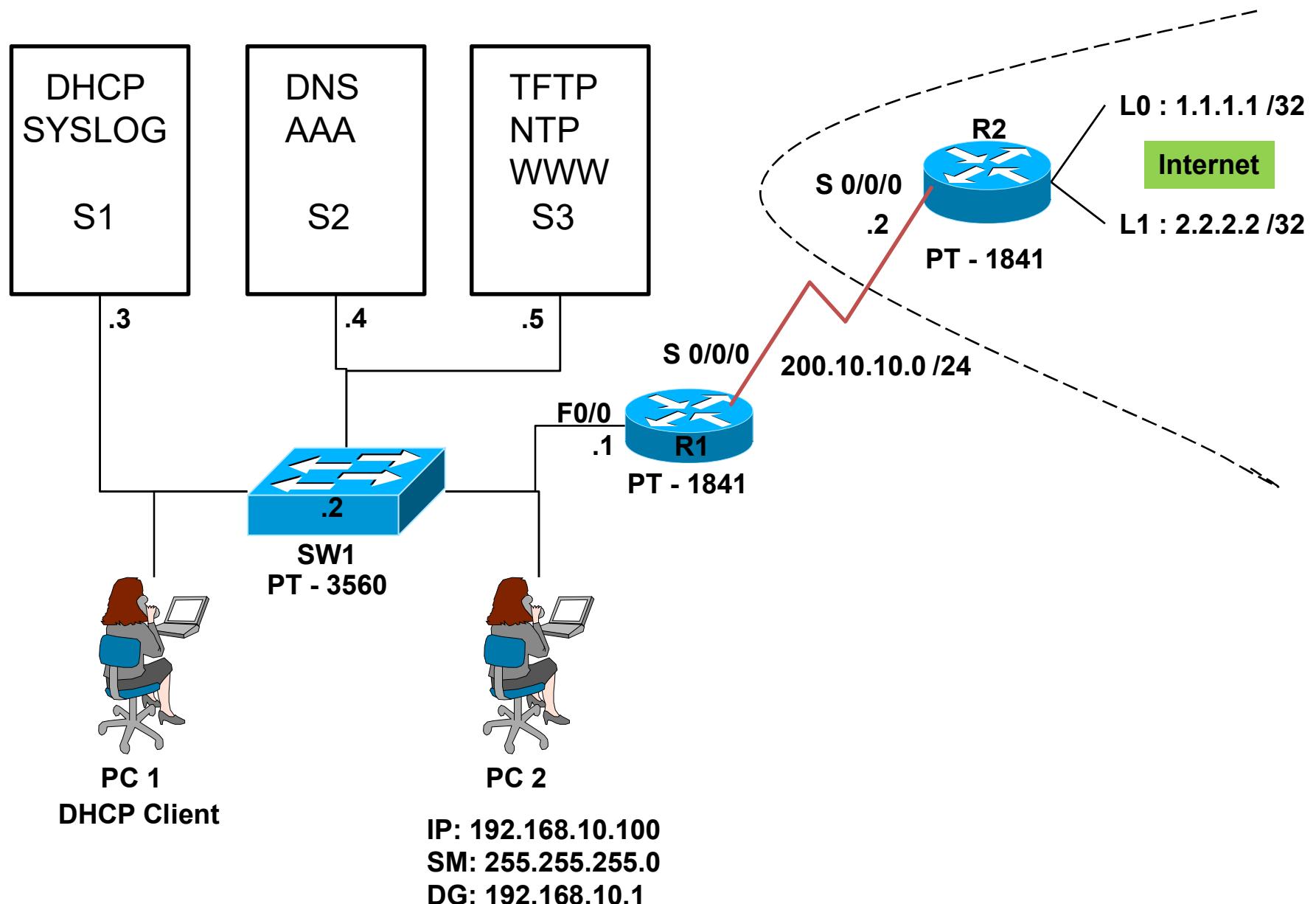
Lesson 22



NTP - LAB Concepts

0. Topology
1. Host Names
2. Ip address
3. Serial
4. Routing protocol
 1. RIP
5. NTP
 1. Service NTP server
 2. Devices : R1
 1. Config NTP Client Configuration
 3. Verify clock details

NTP- Topology

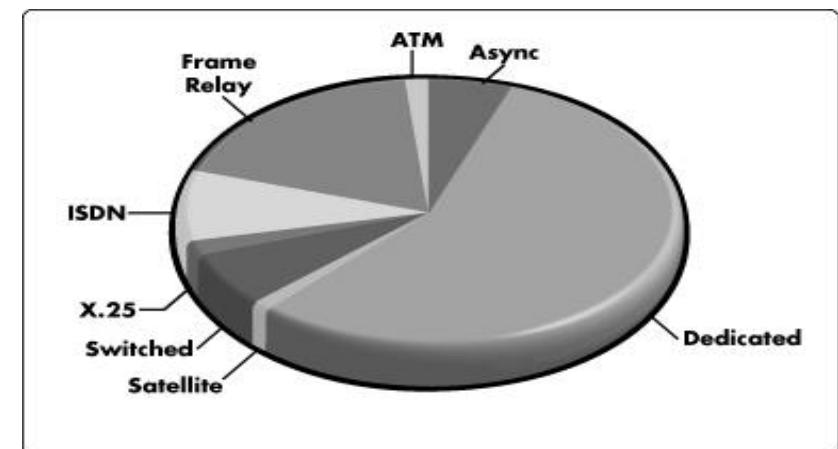


NTP - Commands

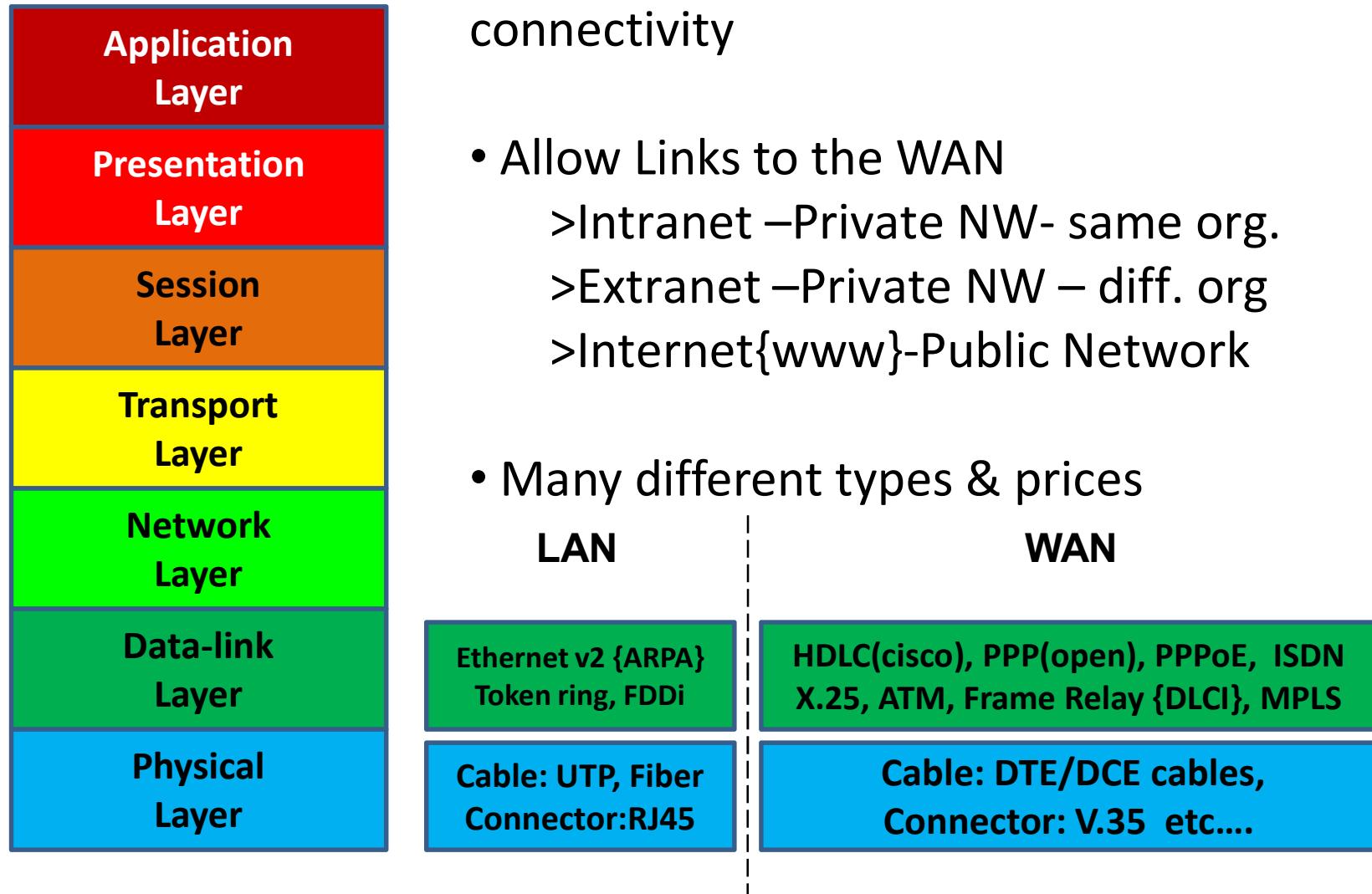
- To configure NTP
 - R1(config)# ntp server 192.168.10.5
 - R1(config)# ntp authenticate
- To verify
 - R1# show clock

WAN Technologies Basics

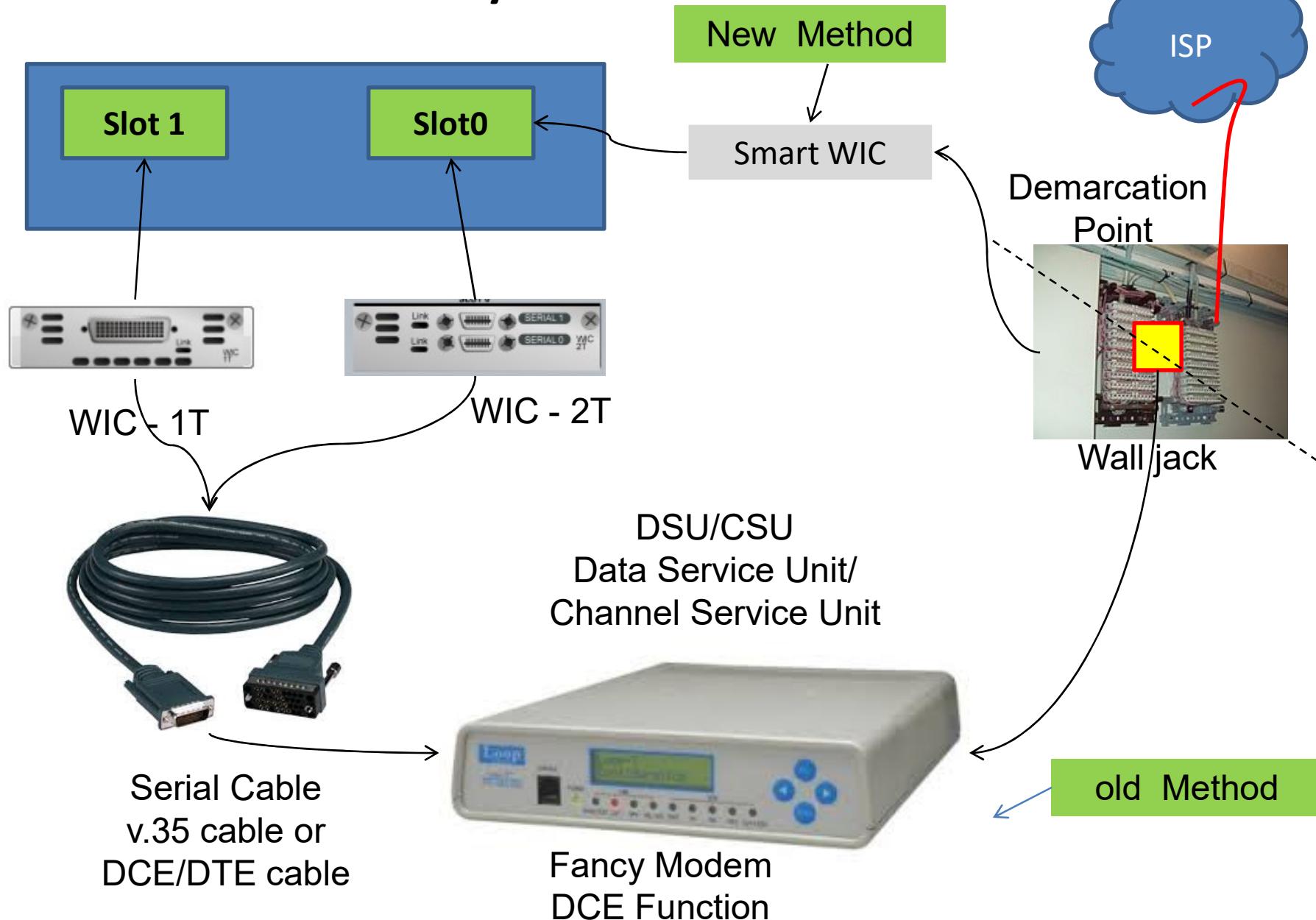
Lesson 44



The Place of WAN Connections



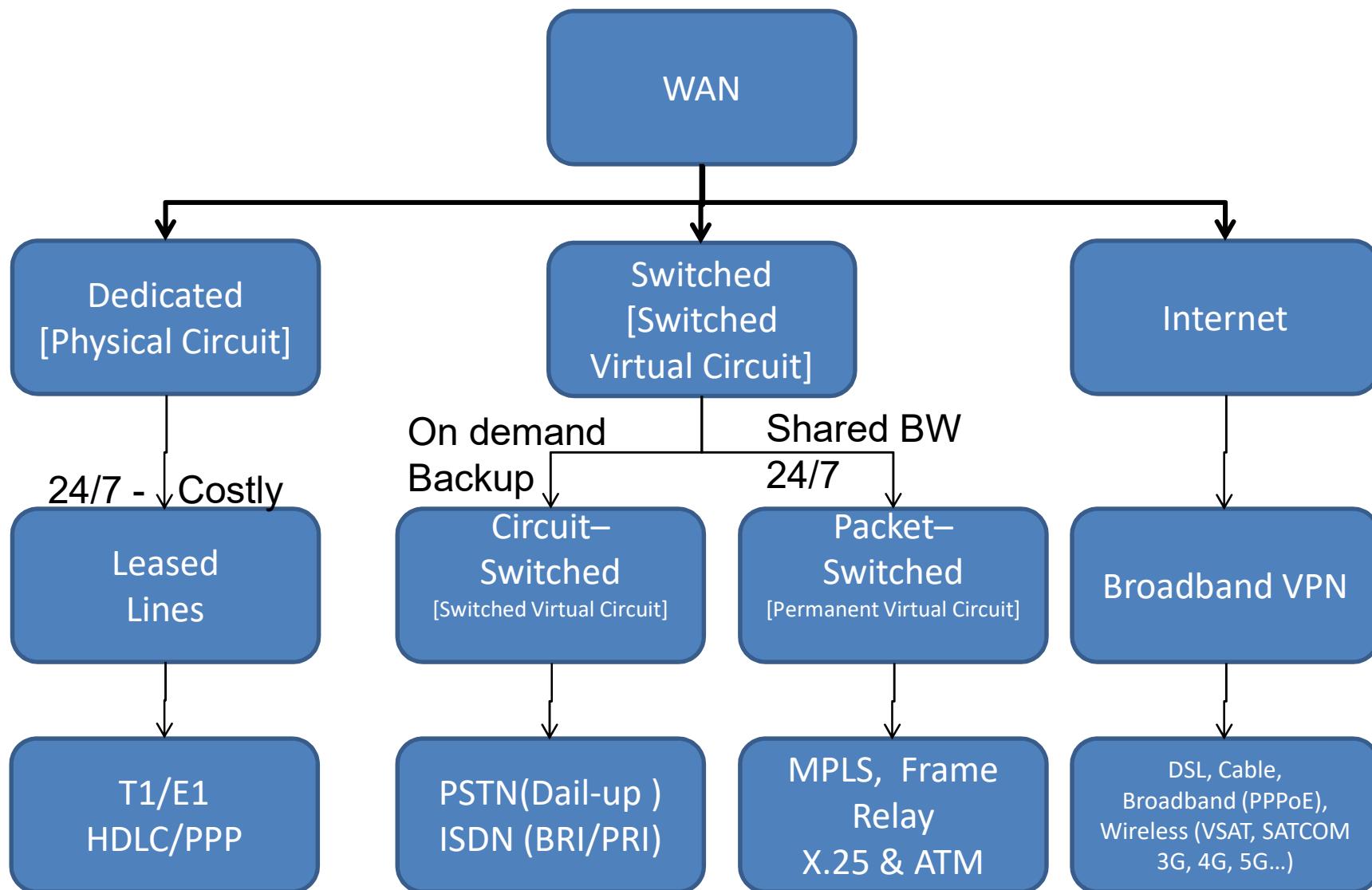
The Physical side of WAN



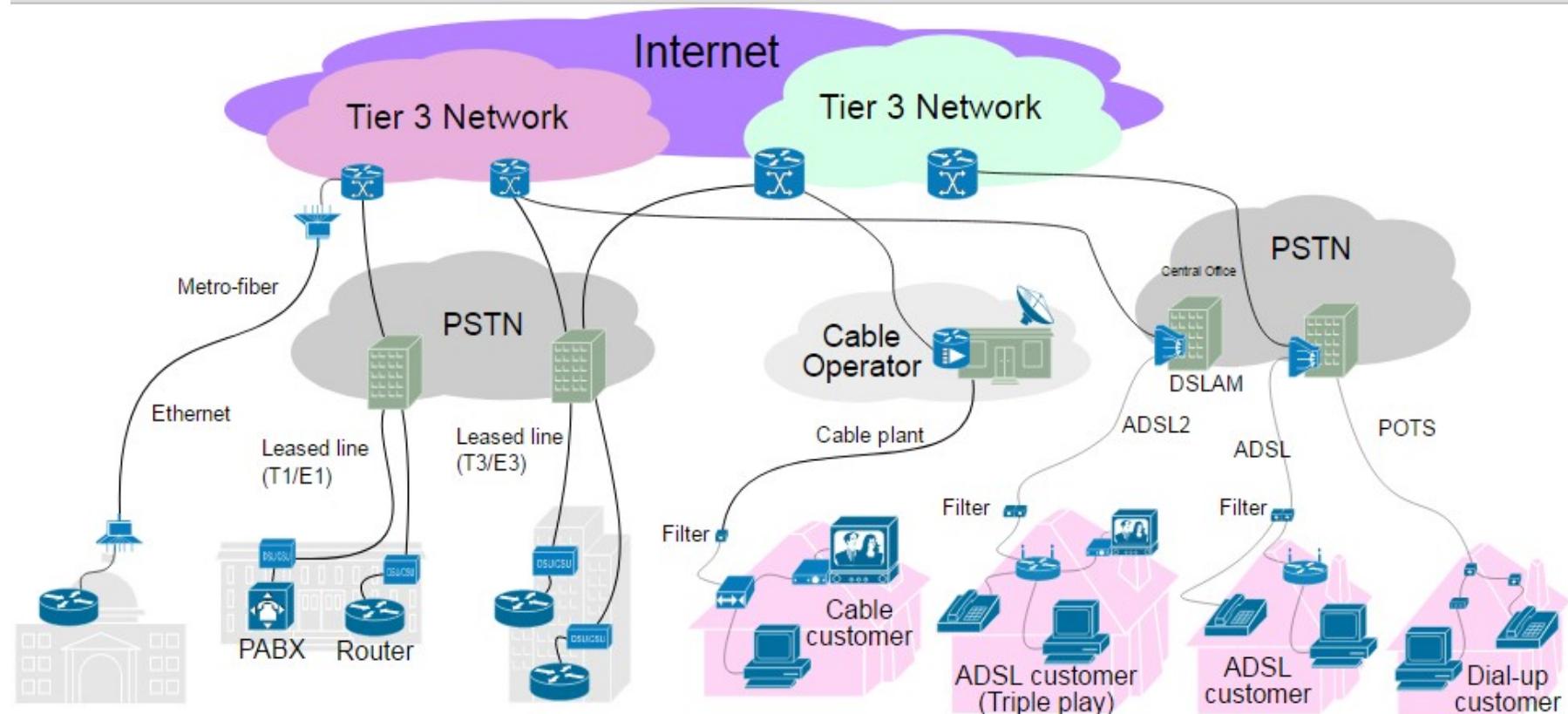
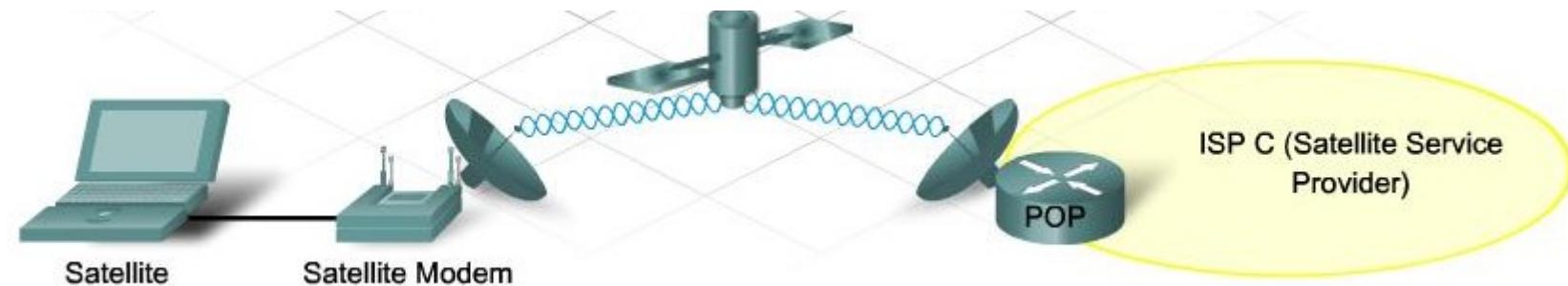
Types of WAN Lines - Connections

- Leased Lines
 - Dedicated Bandwidth between Locations
 - L2 Protocols: HDLC & PPP {PAP, CHAP, MLPPP & PPPoE}
 - Ports:
 - T1 = 1.544 Mbps
 - T3 = 44.736 Mbps
 - E1 {Europe} = 2.048 Mbps
 - Y1 {Japan} = 2.048 Mbps
 - E3 {Europe} = 34.064 Mbps
- Circuit Switching Lines
 - On Demand Bandwidth between Location
 - Examples: Dial-up modems, ISDN
- Packet Switching Lines
 - Shared, But Guaranteed bandwidth between Locations
 - Examples: Frame Relay, ATM, MPLS etc...

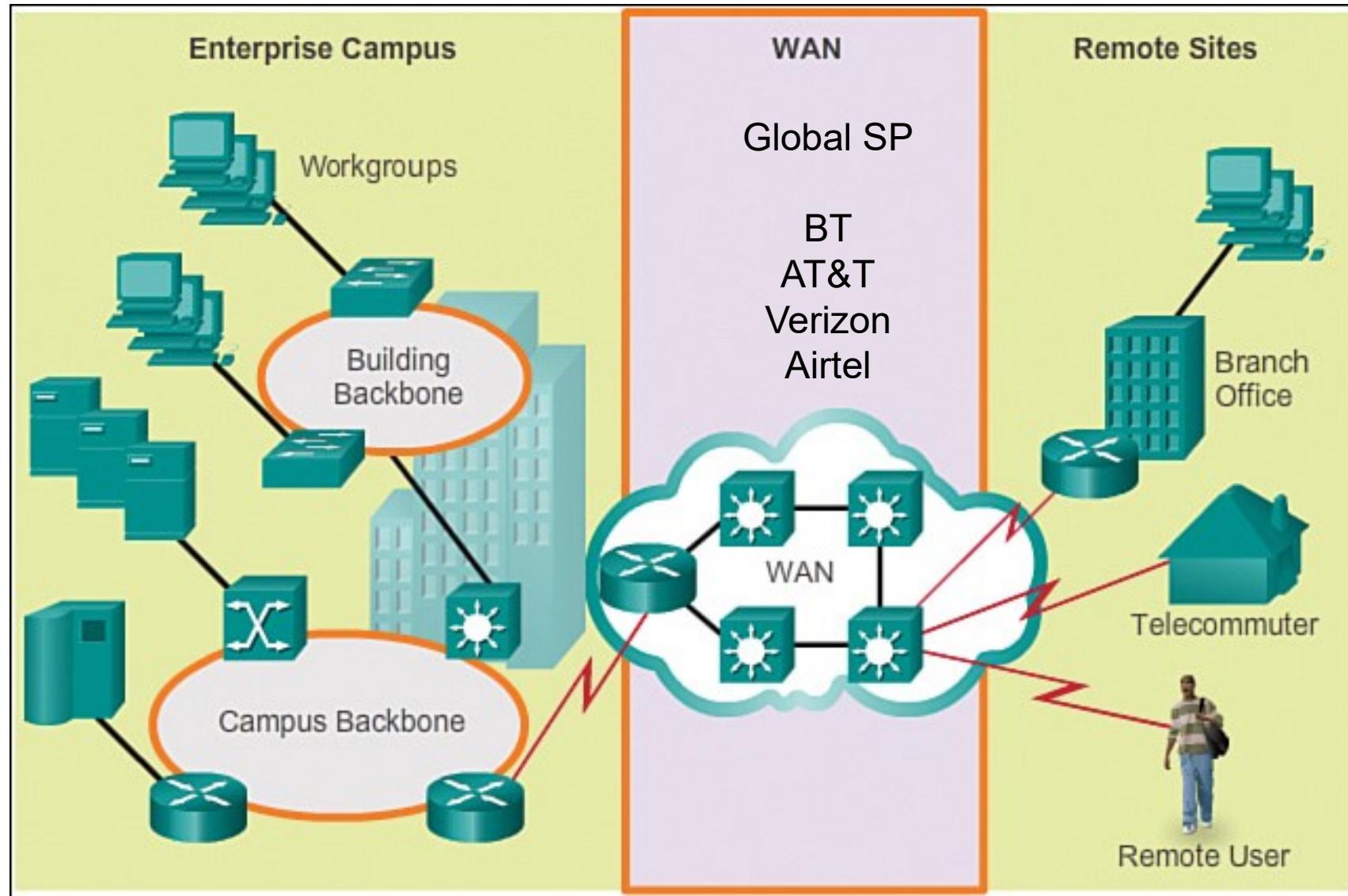
Private WAN Connectivity options



Public WAN Connectivity options

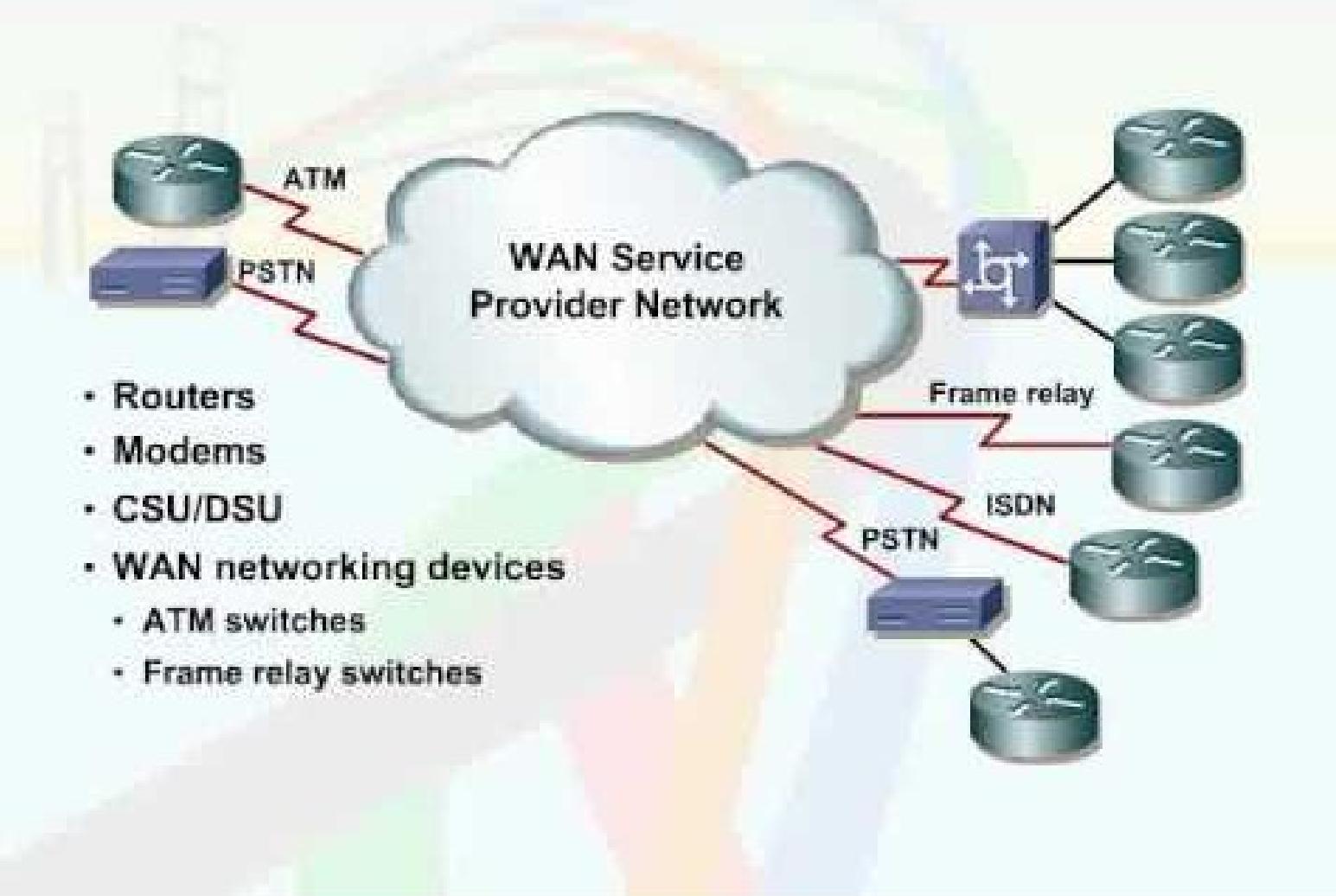


Intro WAN

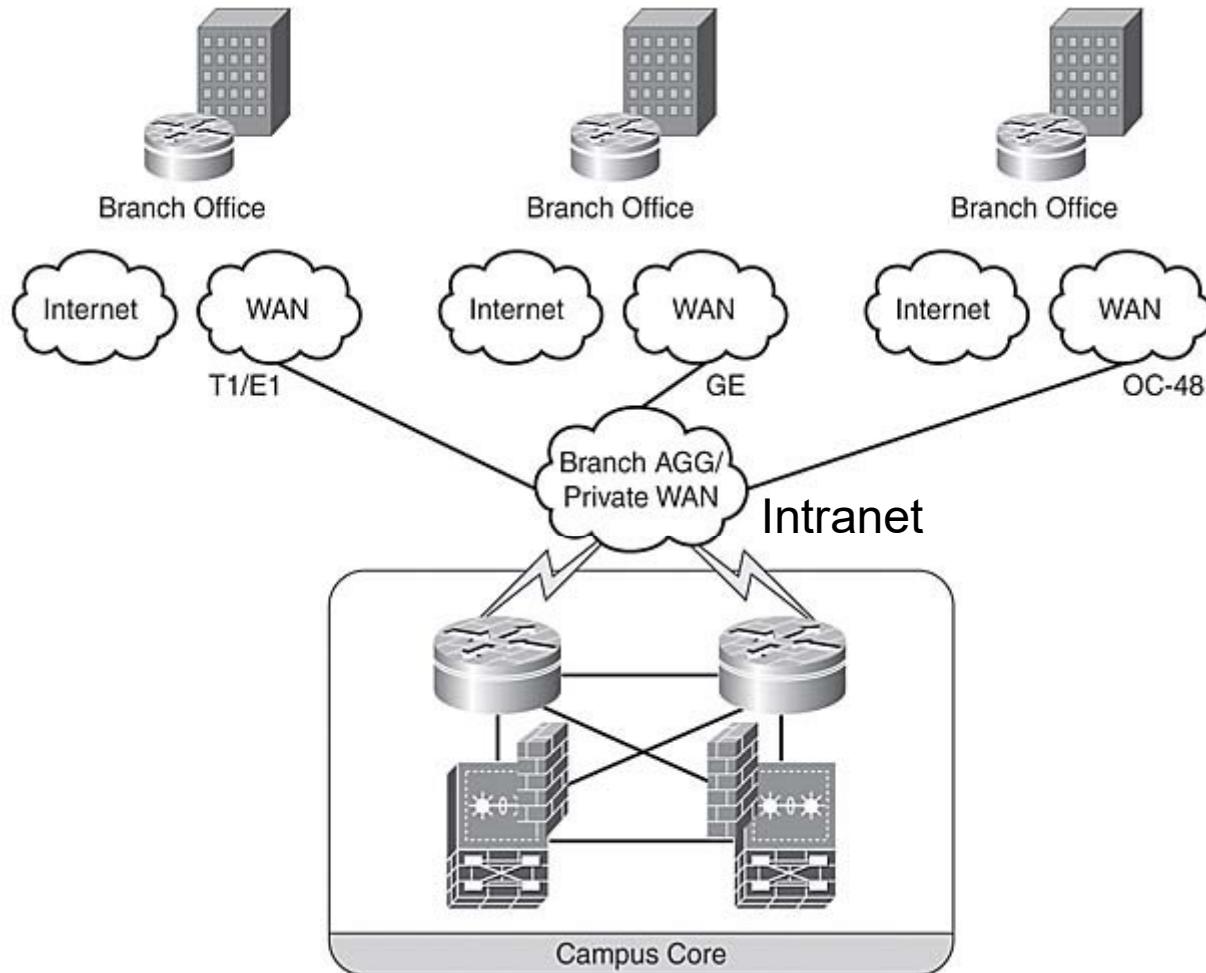


WAN Technologies

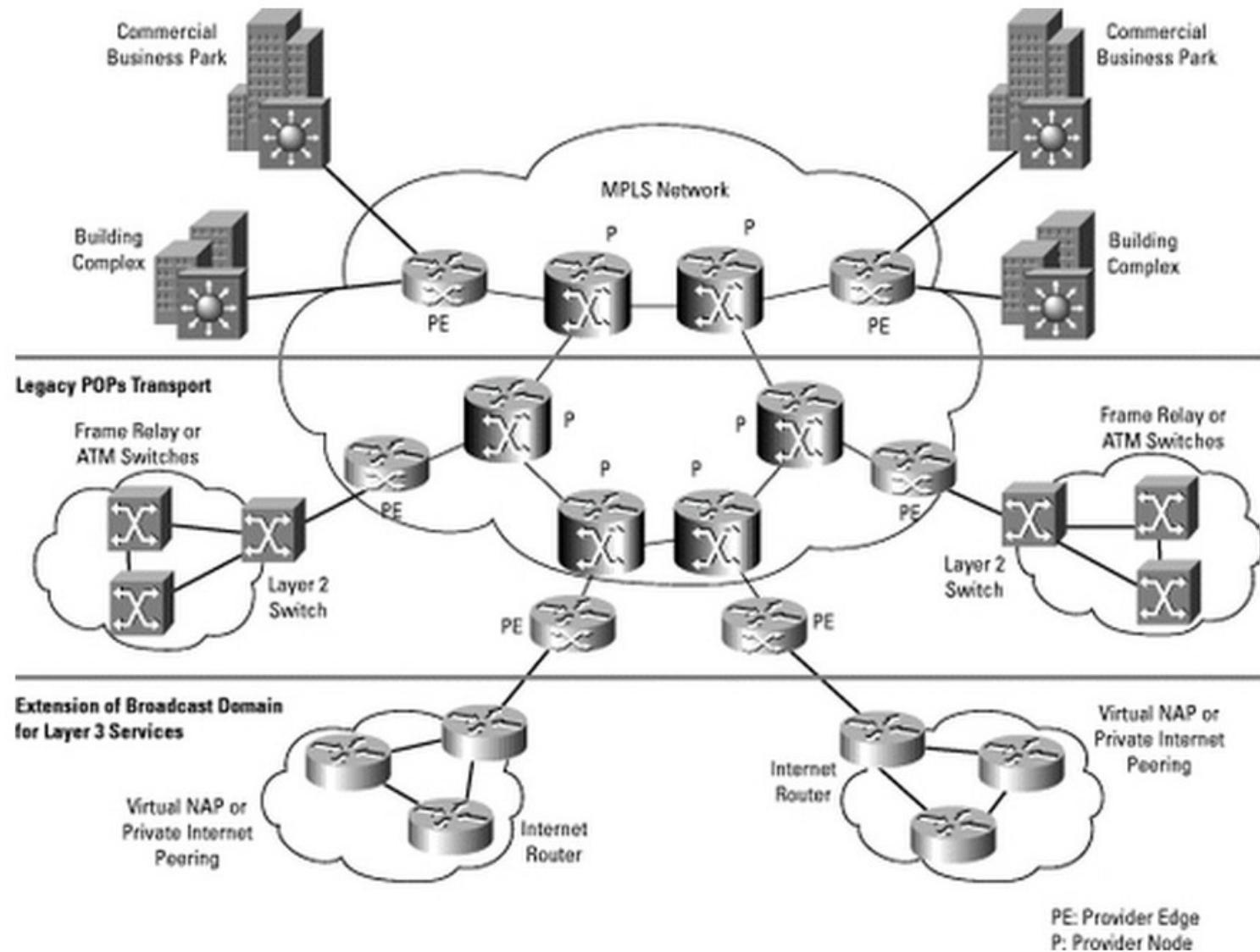
WAN Technologies and Devices



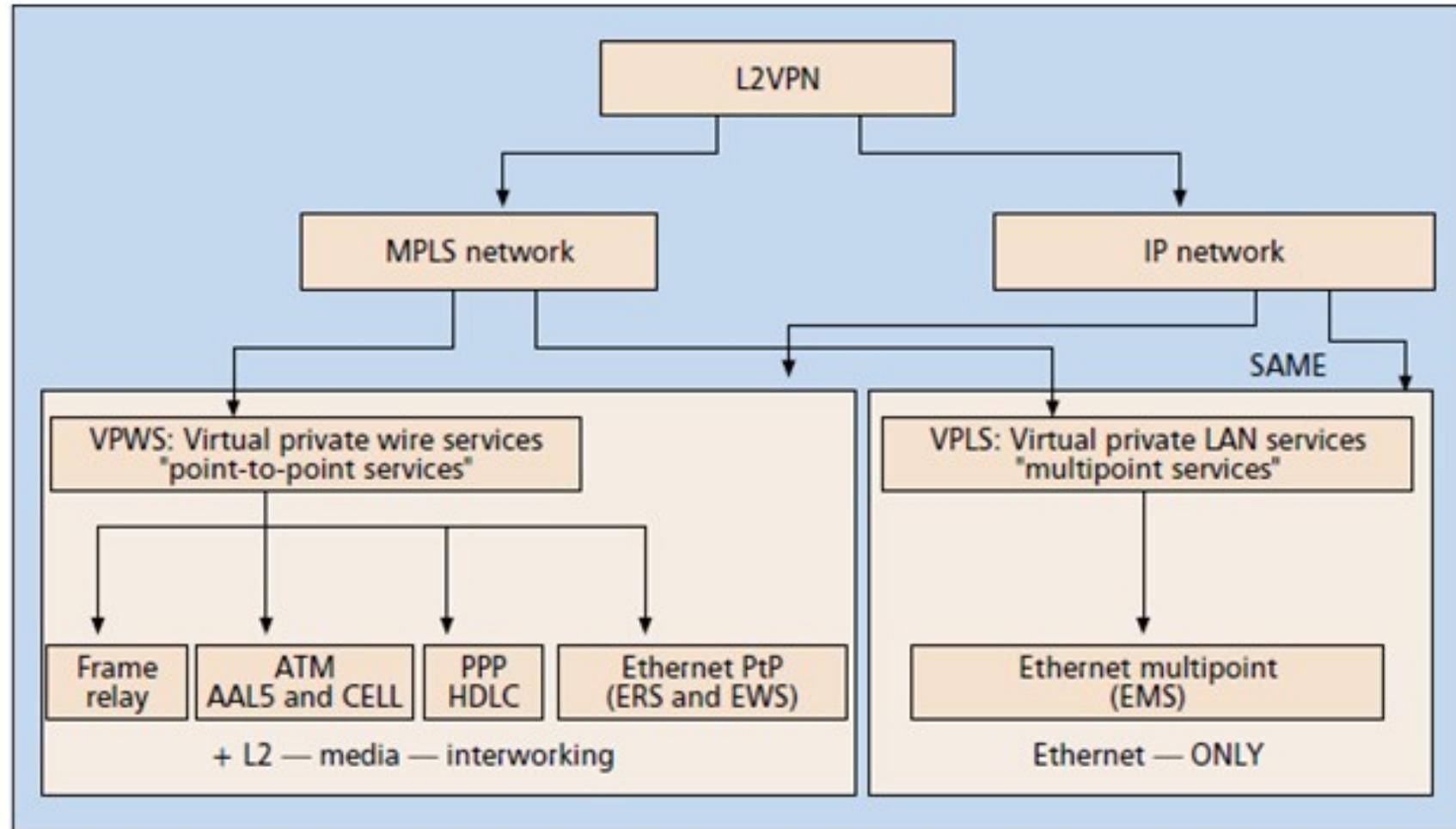
WAN Technologies



WAN Technologies –L2/L3 MPLS VPN



WAN Technologies –L2MPLS VPN

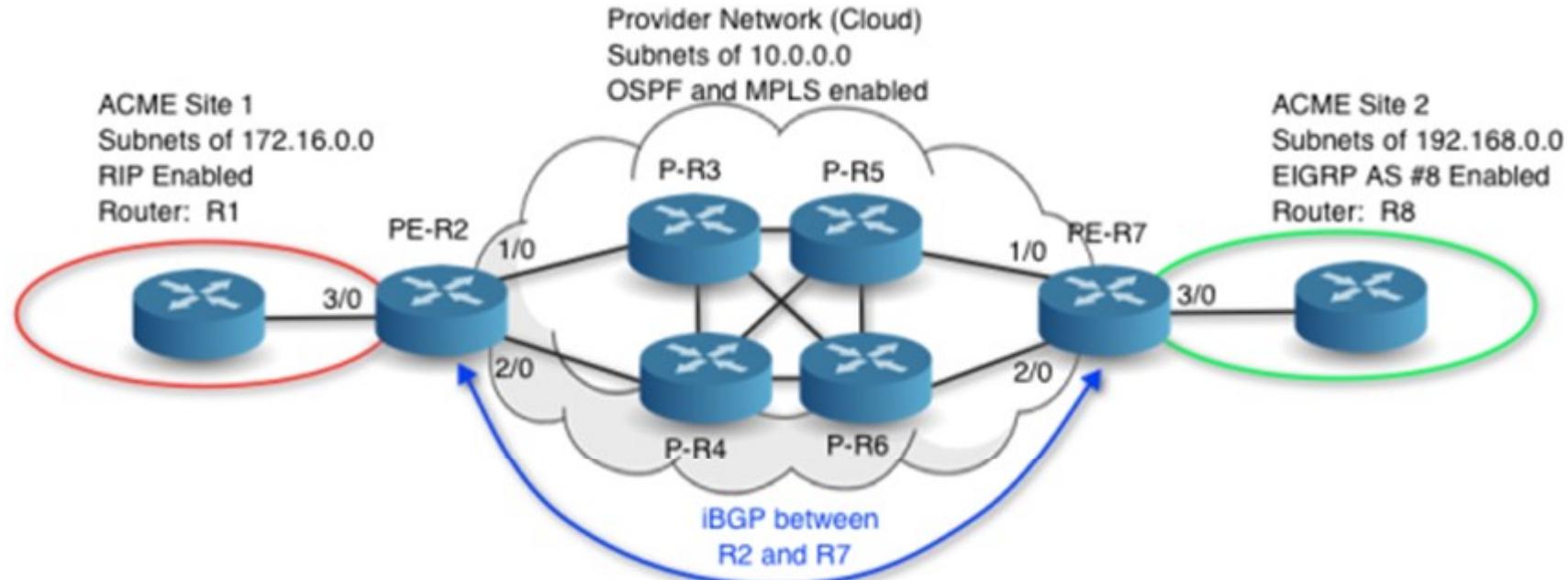


L2 MPLS Configuration steps in Cisco (CE)

Enable – configure terminal – interface type number – no ip address [ip-address mask] [secondary] – negotiation auto – service instance si-id Ethernet – encapsulation dot1q – vlan-id – bridge-domain bd-id – end



WAN Technologies –L3MPLS VPN

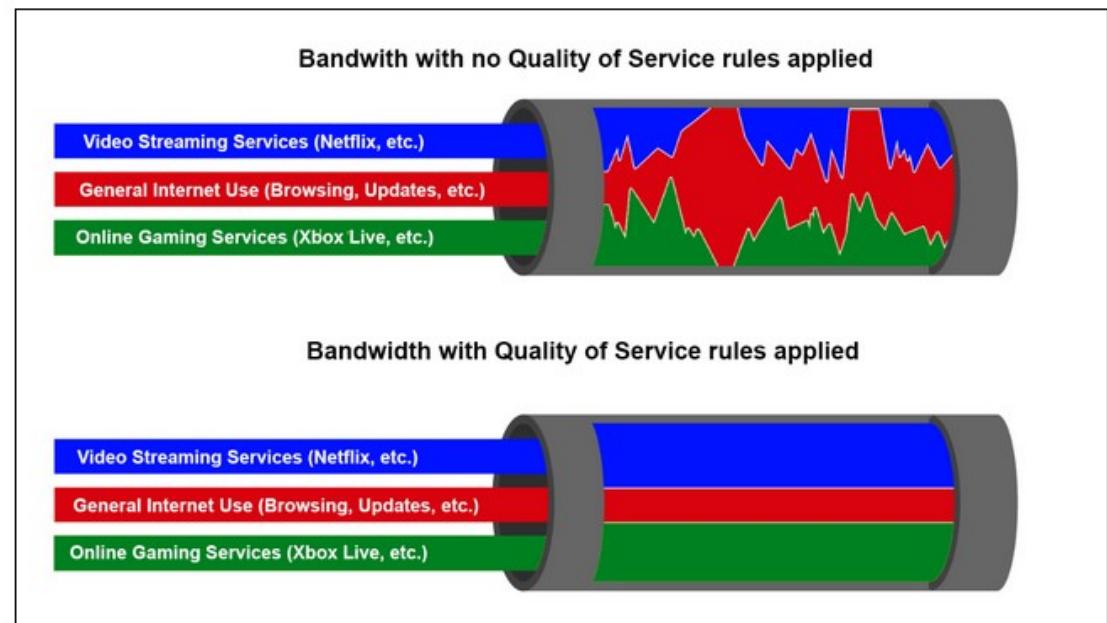


Minimal routing entries at CE site must be done for the configuration of BGP or OSPF to communicate with PE.

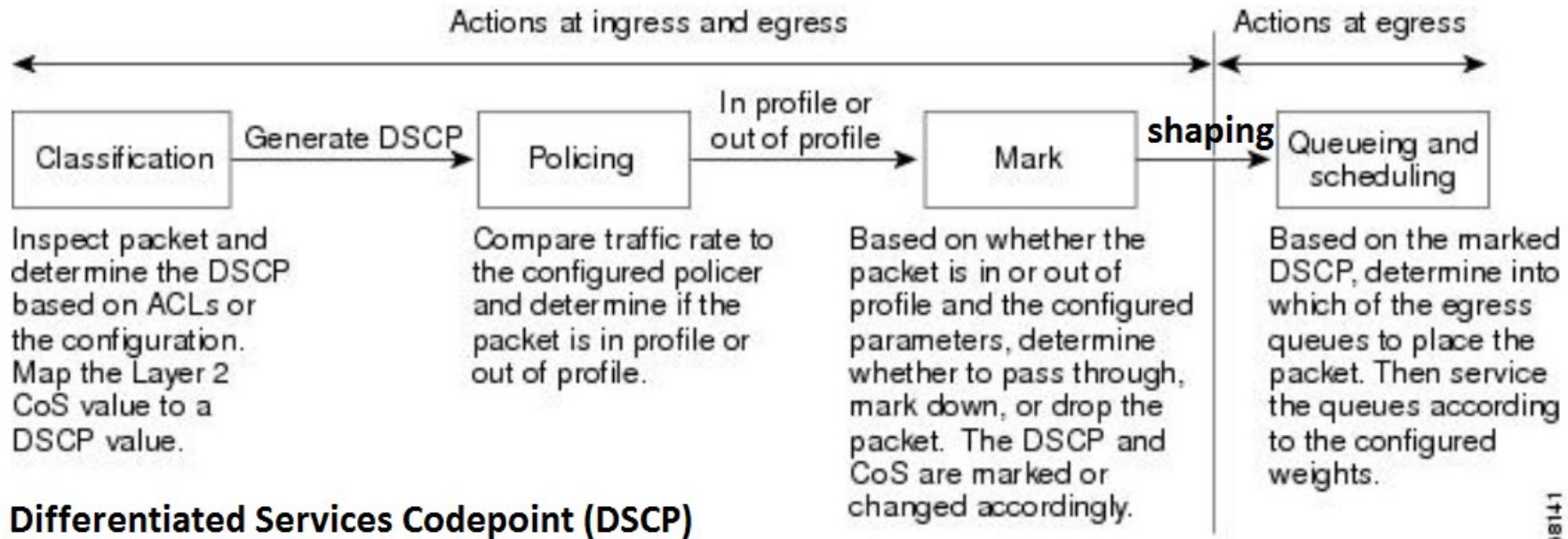
As L3 VPN connected with provider routers to maintain IP forwarding table for each VPN through virtual forwarding table (VRF) makes it less secure and speed down issue may be faced by customers.

WAN Technologies

Quality Of Service {QOS}



QoS



Differentiated Services Codepoint (DSCP)

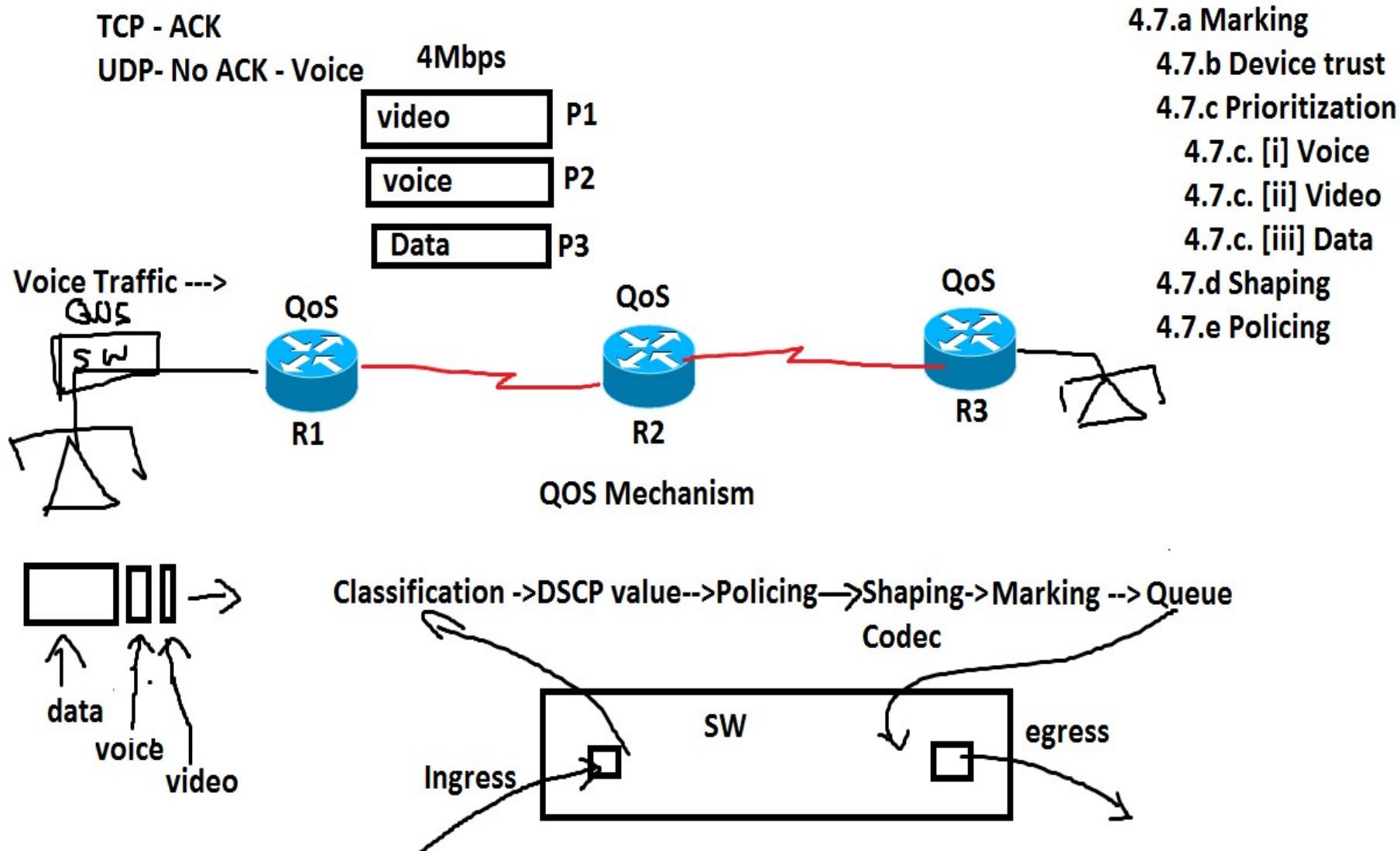
DSCP

Platinum	0
Gold	1
Silver	2
Bronze	3

148

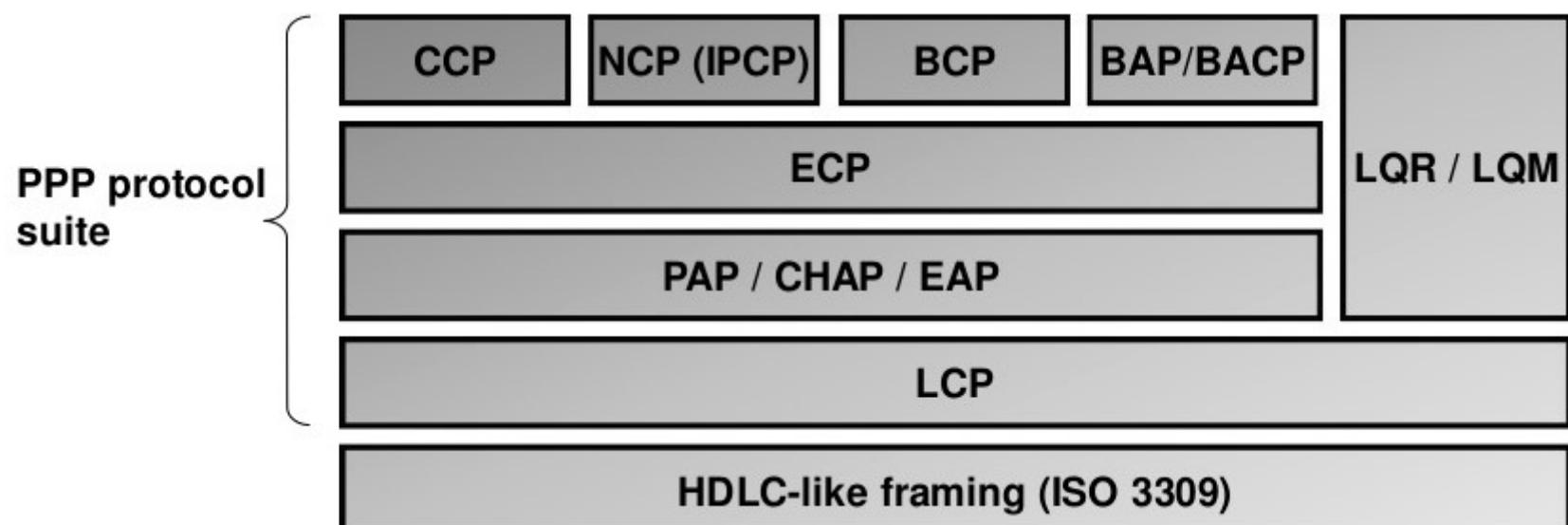


QoS

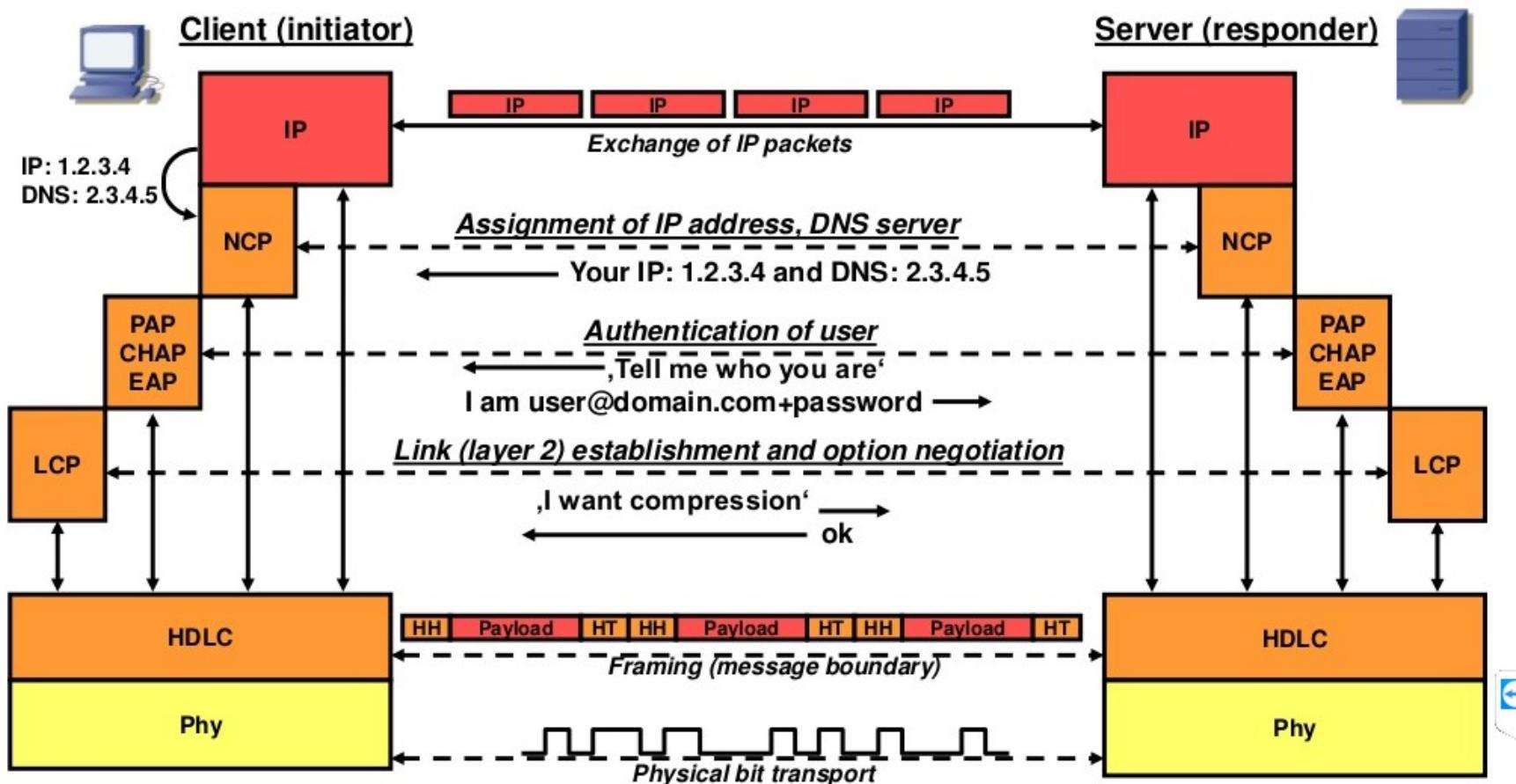


WAN Technologies

PPP

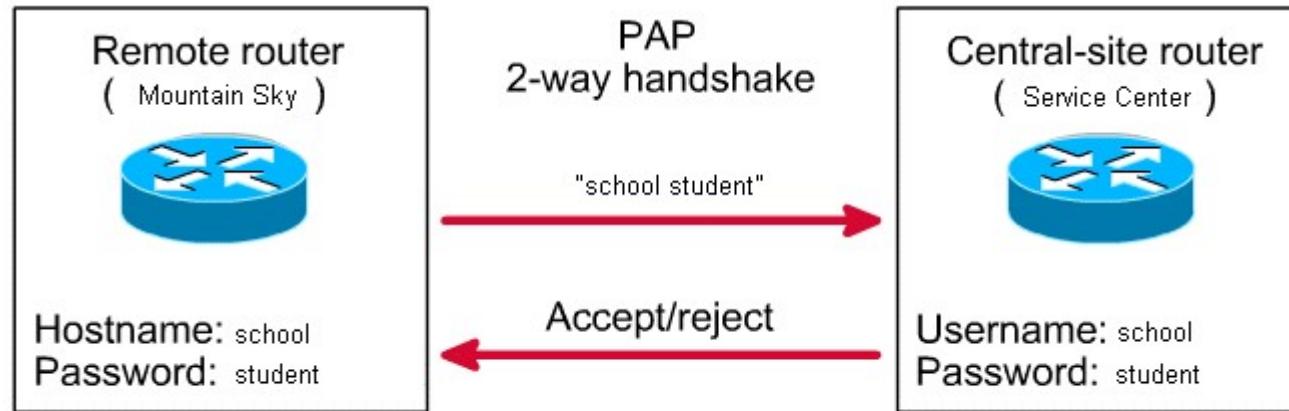


PPP Protocol Suite

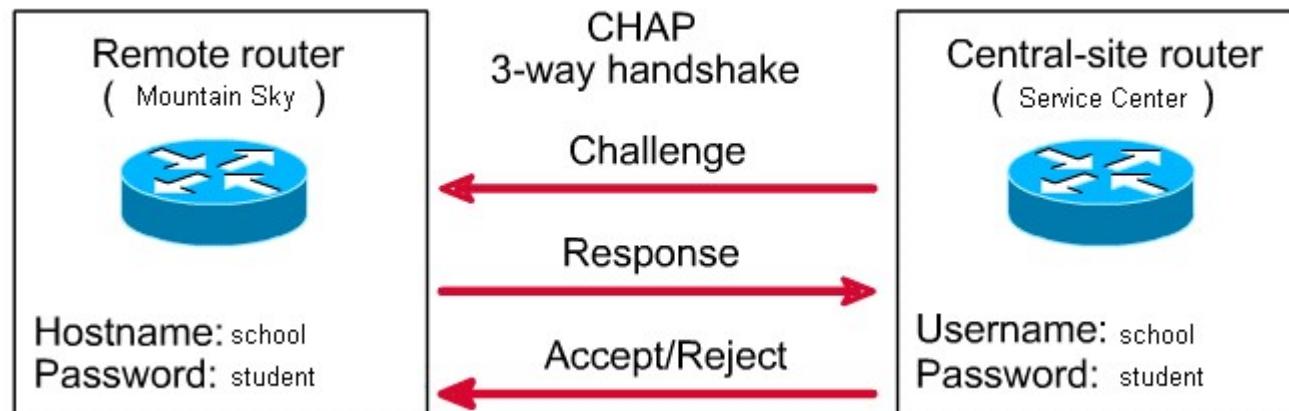


PAP vs. CHAP

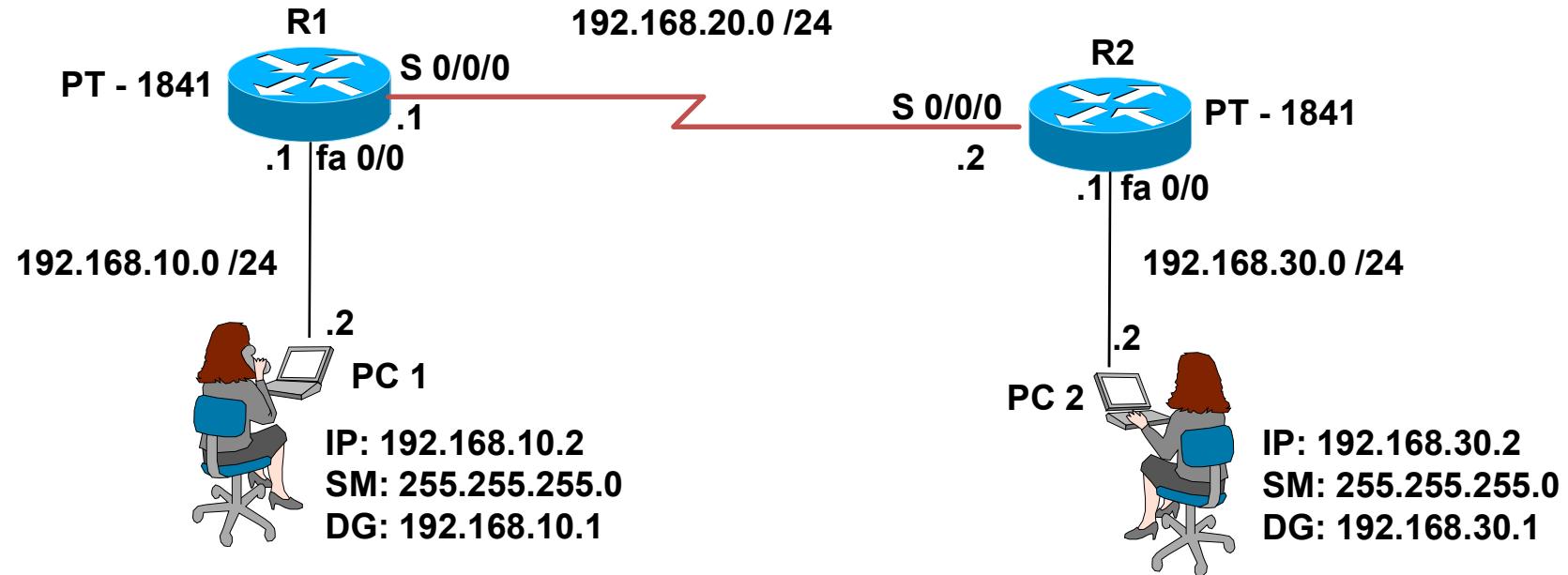
Plain text Authentication Protocol



Challenge Handshake Authentication Protocol



PPP & CHAP – Topology & Commands



Configure uN & PSSWD:

```
R1(config)#username R2 password cisco
```

Configure PPP:

```
R1 (config-if)# encapsulation ppp
```

Configure PPP:

```
R1 (config-if)# ppp authentication chap
```

To Verify:

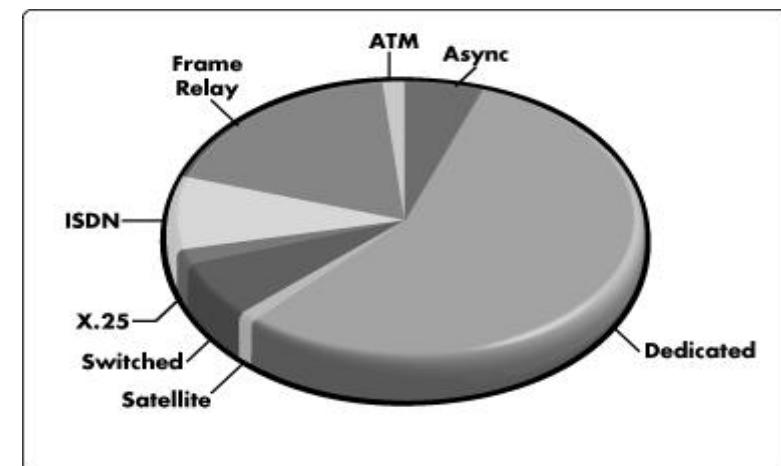
```
R1 # show interface s0/0/0
```

```
R1# show ip int brief
```

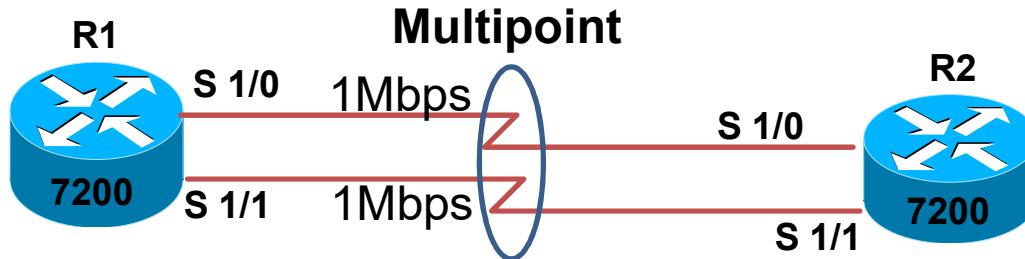


WAN Technologies

MLPPP



MLPPP – Concept/Topology/commands



Interface Multilink1

```
ip add 192.168.1.1 255.255.255.0
ppp multilink
ppp multilink group 1
```

```
interface Serial1/0
encapsulation ppp
ppp multilink
ppp multilink group 1
!
interface Serial1/1
encapsulation ppp
ppp multilink
ppp multilink group 1
```

Interface Multilink 1

```
ip add 192.168.1.2 255.255.255.0
ppp multilink
ppp multilink group 1
```

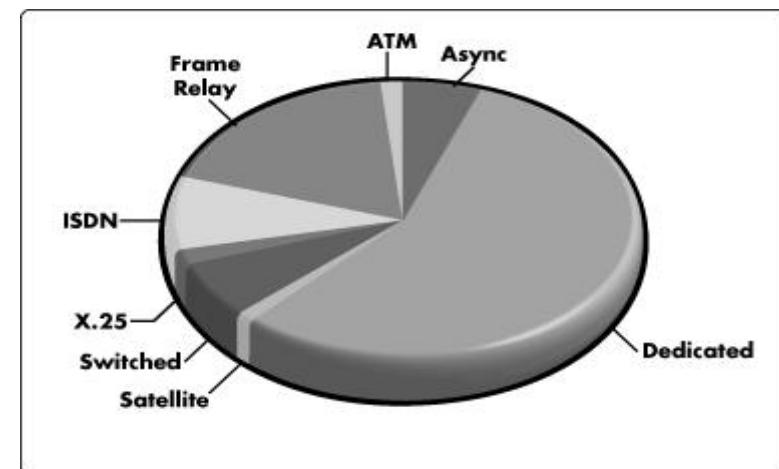
```
interface Serial1/0
encapsulation ppp
ppp multilink
ppp multilink group 1
!
interface Serial1/1
encapsulation ppp
ppp multilink
ppp multilink group 1
```

To verify:

R1# show ppp multilink

WAN Technologies

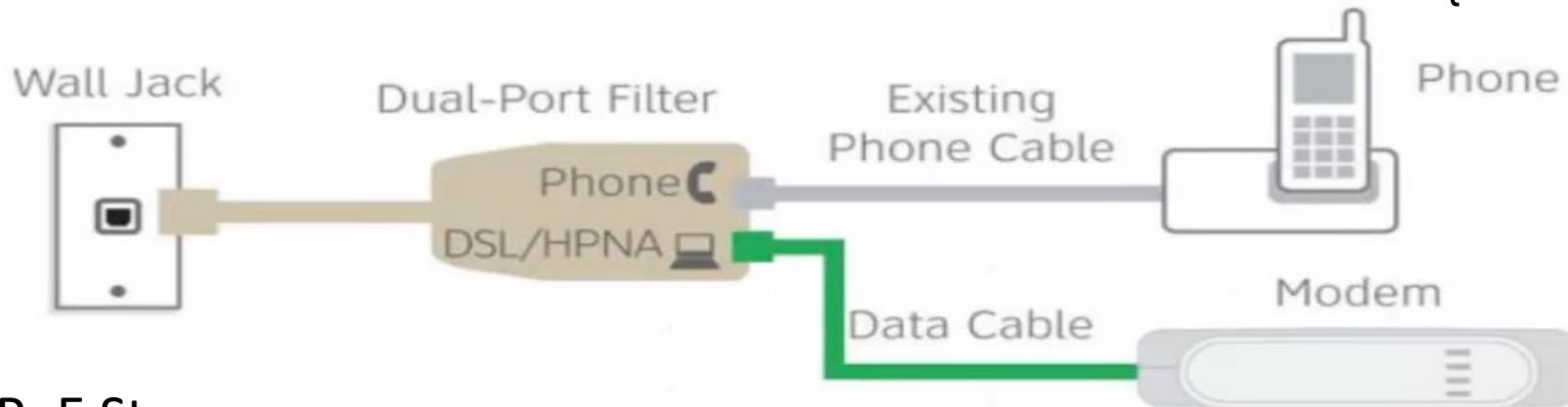
Point-to-Point Over Ethernet {PPPoE}



PPPoE (client side only)

PPPoE = Point to Point Over Ethernet

>>>Ability to connect a network of hosts to Remote Access Server {RAS} [also called as Network Access Server or Broadband Remote Access Server {B-RAS}]



PPPoE Stages:

1. Discovery Stage {5 sub states}
 1. PPPoE Active Discovery Initiation {PADI} Packet
 2. PPPoE Active Discovery offer {PADO} packet
 3. PPPoE Active Discovery Request {PADR} Packet
 4. PPPoE Active Discovery Session-Configuration {PADS} Packet
 5. PPPoE Active Discovery Terminate {PADT}
2. PPP Session Stage

Reference: http://en.wikipedia.org/wiki/Point-to-point_protocol_over_Ethernet#PPP_session



kumar6009@gmail.com



@air.ds2

Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3 379

PPPoE Concept

0. Topology {GNS 3 - 7200 as PPPoE server & Client}

1. Configure PPPoE Server {5 Steps}

1. Bba-group
2. Virtual-templates interface configuration
3. IP Local Pool
4. Customer Credentials
5. Attach Bba-group to Physical Interface

2. Configure PPPoE Client

1. Dialer
 1. IP Address, Encapsulation, Authentication,
 2. Dialer pool, Dialer-group & MTU =1492
2. Dialer-list
3. Default route
4. Attached the physical interface to dialer pool

3. Loopback & PAT

1. Server : L0 – 8.8.8.8/24
2. Client : L0 – 192.168.1.1/24

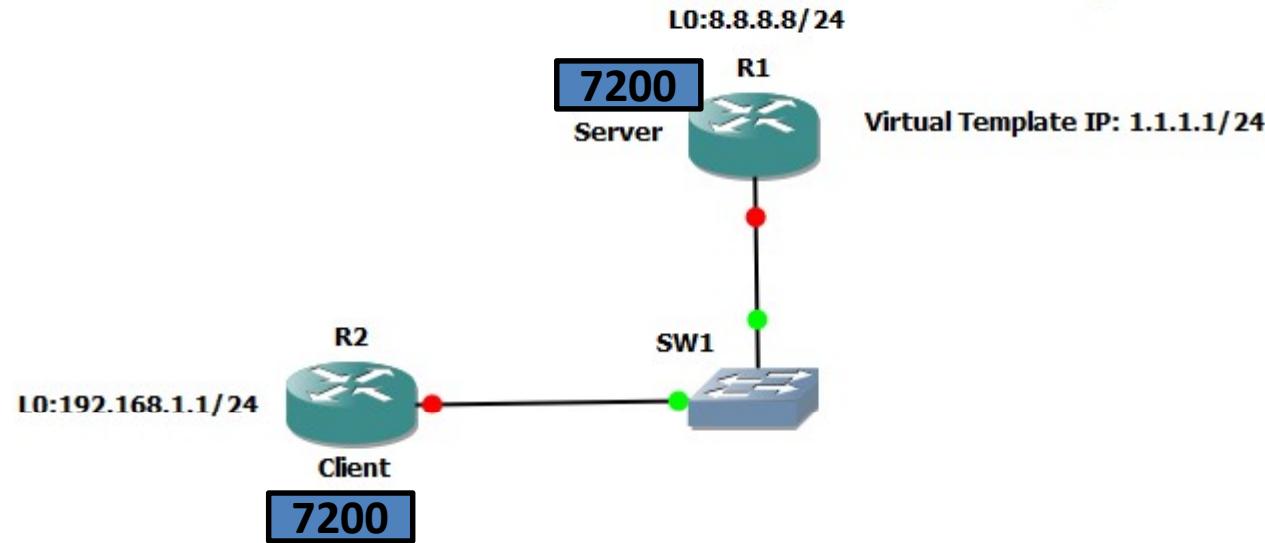
4. Verify i.e. Client

1. Show ip interface brief i.e. dialer - 1.1.1.2 – 1.1.1.254
2. Ping 8.8.8.8 source loopback 0
3. Show ip nat translations



PPPoE Topology

PPPoE Server & Client Configuration



PPPoE Commands

- ISP Server Configuration: Bba-group
 - R1(config)# bba-group pppoe customer
 - R1(config)# virtual-template 1
 - R1(config)# exit
- ISP Server Configuration: Virtual Template Creation
 - R1(config)# Interface virtual-template 1
 - R1(config-if)# ip address 1.1.1.1 255.255.255.0
 - R1(config-if)# no shut
 - R1(config-if)# peer default ip address pool test_pool
 - R1(config-if)# ppp authenticaton chap callin
- ISP Server Configuration: IP Pool Creation
 - R1(config)# ip local pool test_pool 1.1.1.2 1.1.1.254
- ISP Server Configuration: User Credentials
 - R1(config)# username R2 password cisco
 - R1(config)# username R3 password cisco
- ISP Server Configuration: Attach Physical interface to bba group
 - R1(config)# interface fastethernet 0/0
 - R1(config-if)# pppoe enable group customer
 - R1(config-if)# no shut

PPPoE Commands

- Client Configuration: Dialer
 - R2(config)# Interface Dailer 1
 - R2(config-if)# ip address negotiated
 - R2(config-if)# encapsulation ppp
 - R2(config-if)# ppp chap password cisco
 - R2(config-if)#dialer pool 1
 - R2(config-if)#dialer-group 1
 - R2(config-if)#ip MTU 1492
 - R2(config-if)#exit
- Client Configuration: Dialer-list
 - R2(config)# dialer-list 1 protocol ip permit
- Client Configuration: Default Route
 - R2(config)# ip route 0.0.0.0 0.0.0.0 dialer 1
- Client Configuration: Attach Dail-pool to Physical Interface
 - R2(config)# interface fastethernet 0/0
 - R2(config-if)#pppoe enable
 - R2(config-if)#pppoe-client dial-pool-number 1

PPPoE Commands

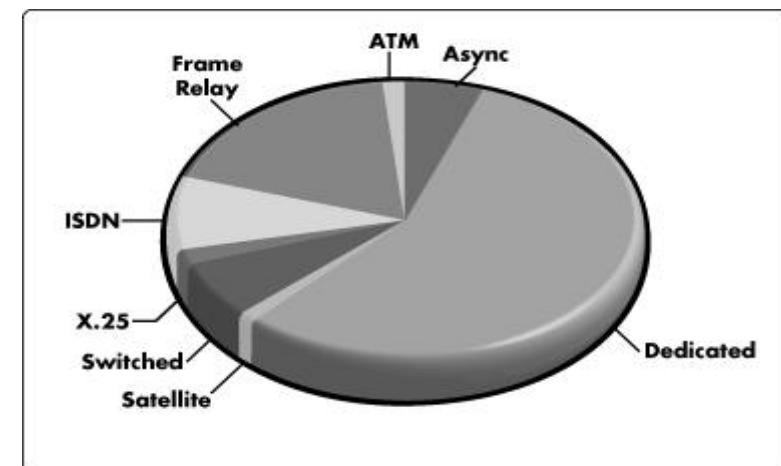
- Client Configuration: Create Loopback
 - R2(config)# Interface Loopback 0
 - R2(config-if)# ip address 192.168.1.1 255.255.255.0
- Server Configuration: Create Loopback
 - R1(config)# Interface Loopback 0
 - R1(config-if)# ip address 8.8.8.8 255.255.255.0
- Client Configuration: PAT
 - R2(config)# interface fasthernet 0/0
 - R2(config-if)#ip nat inside
 - R2(config-if)#exit
 - R2(config)# interface dialer 1
 - R2(config-if)#ip nat outside
 - R2(config-if)#exit
 - R2(config)#ip access-list standard 1
 - R2(config-std-nacl)#permit 192.168.1.1 0.0.0.255
 - R2(config)#ip nat inside source list 1 interface dialer 1 overload

PPPoE Commands

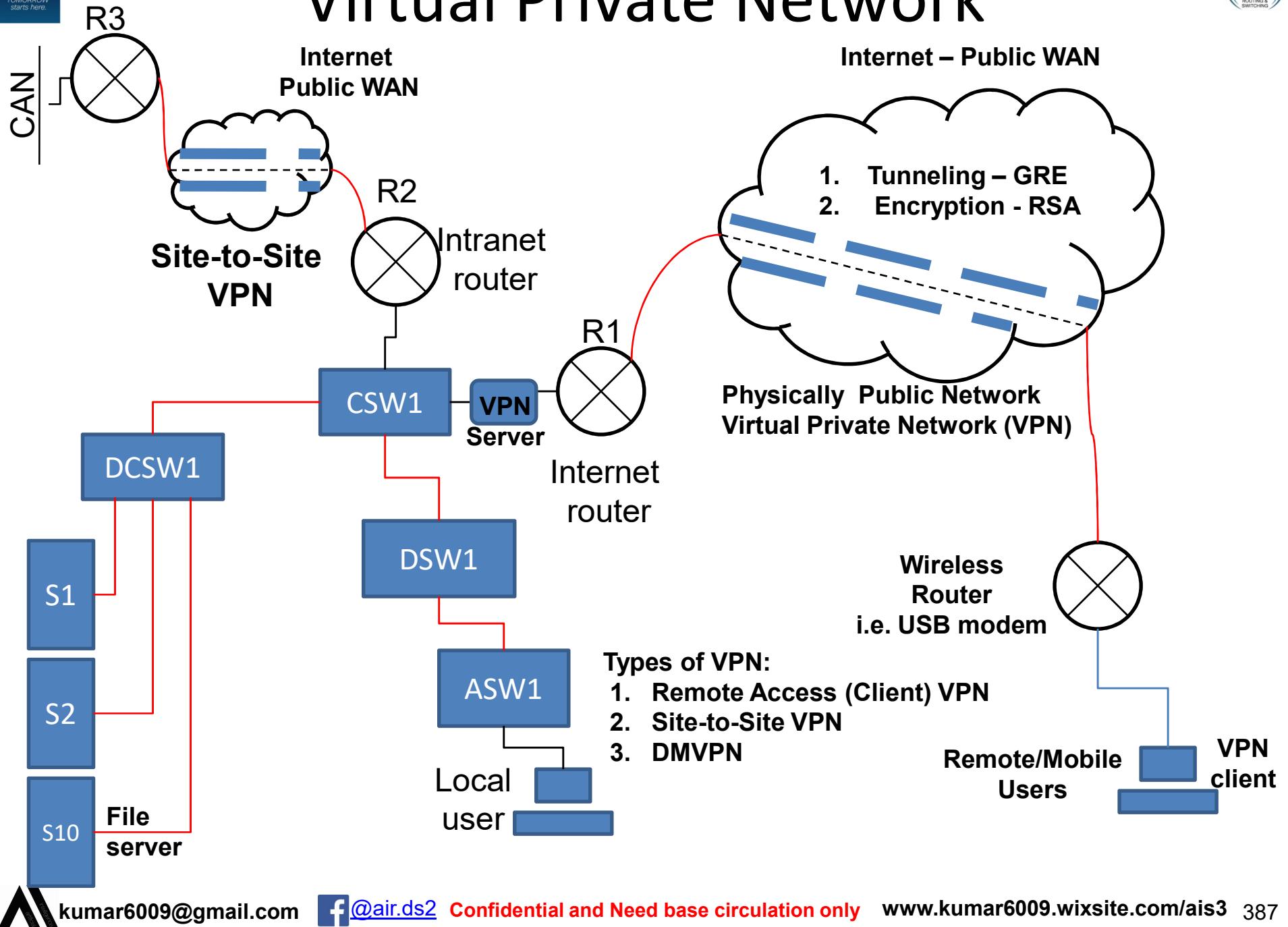
- Verify:
 - R2# show ip interface brief i.e. dailer interface – 1.1.1.2 – 1.1.1.254
 - R2# debug pppoe events
 - R2# debug ppp authentication
 - R2# debug ppp negotiation
 - R2#ping 1.1.1.1
 - R2#ping 8.8.8.8 source loopback 0
 - R2#show ip nat translations

WAN Technologies

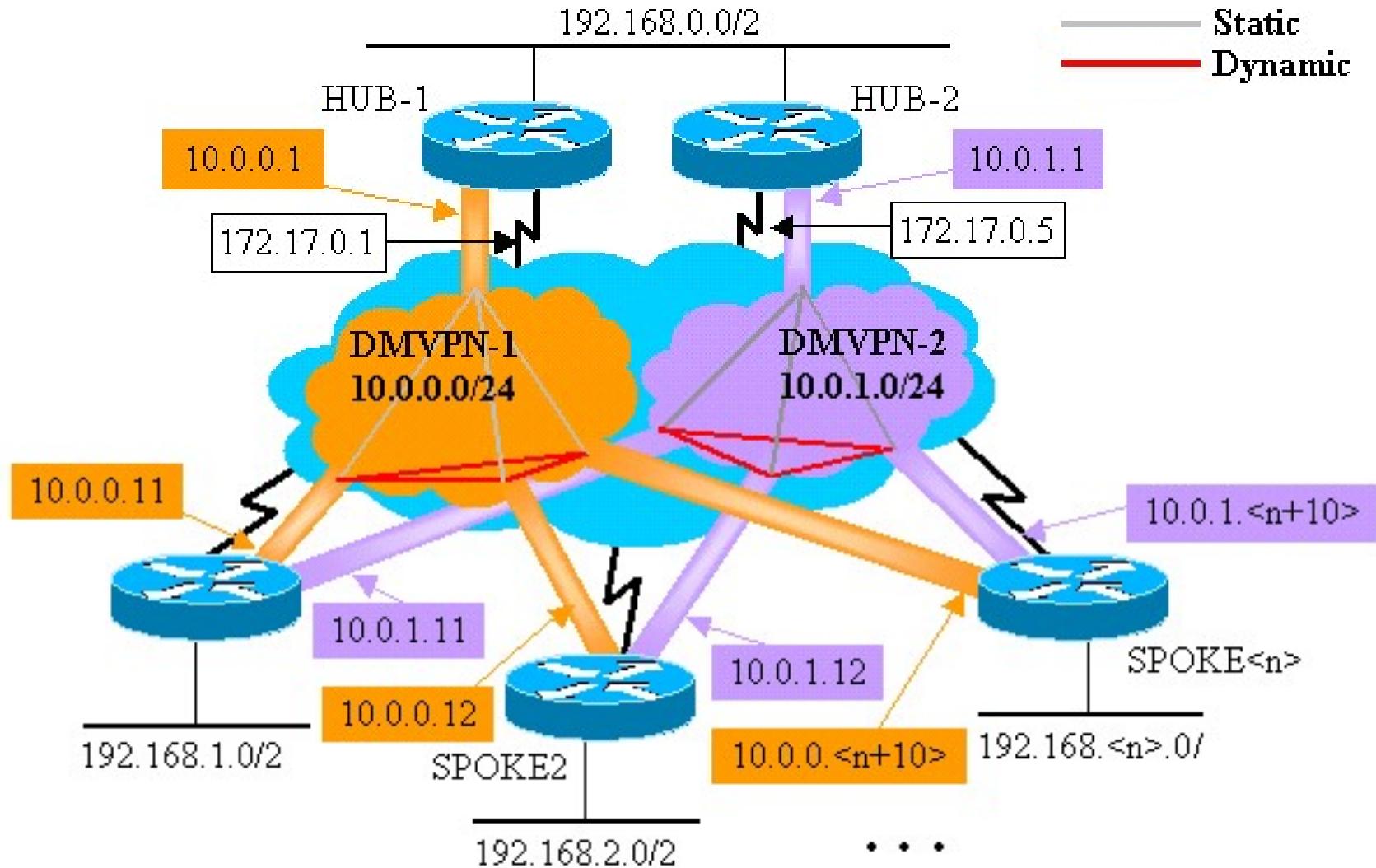
VPN – GRE



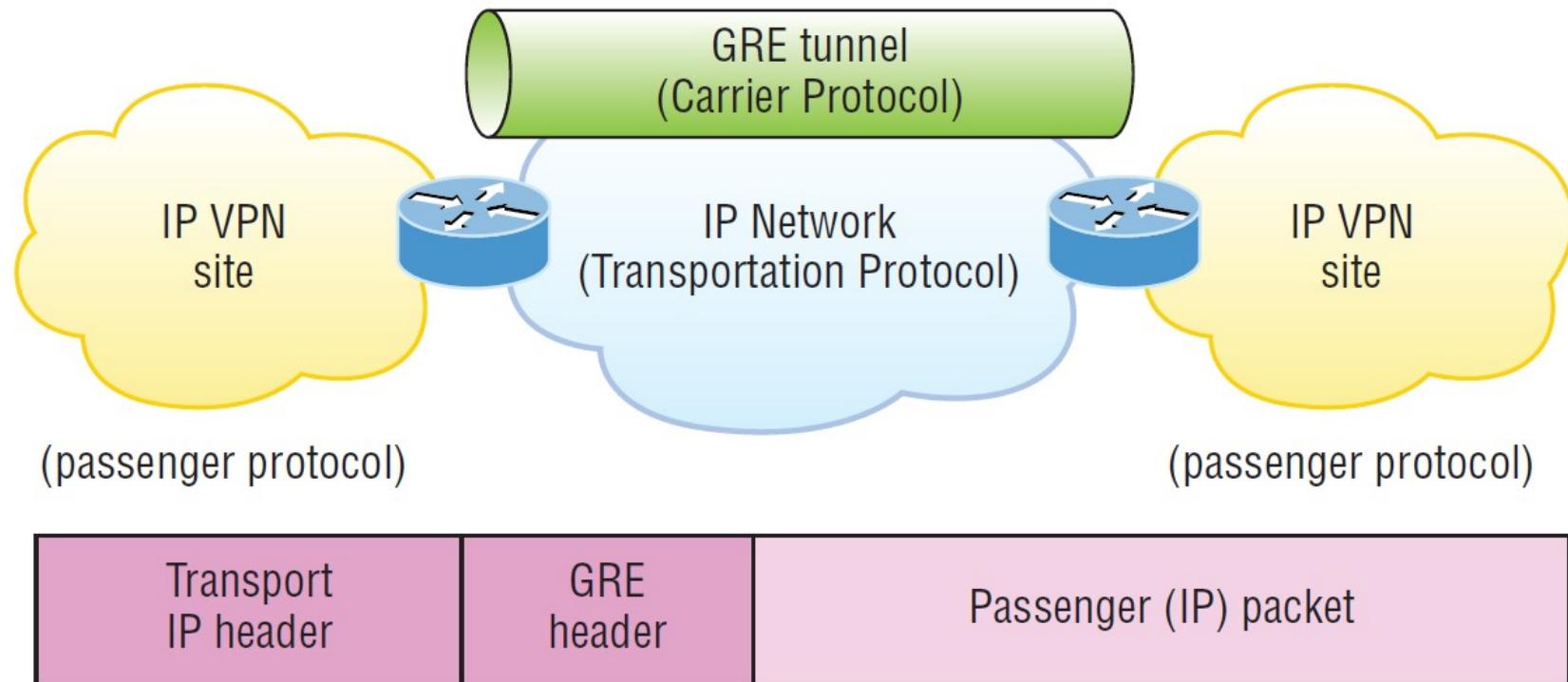
Virtual Private Network



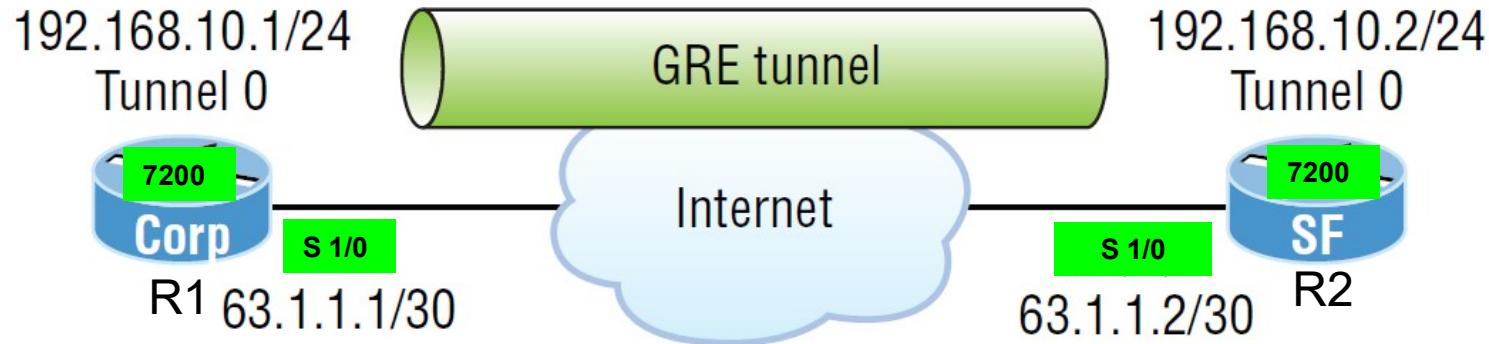
DMVPN - Dynamic Multipoint VPN



Tunneling



GRE tunnel



```
Corp(config)#int s1/0
Corp(config-if)#ip address 63.1.1.1 255.255.255.252
Corp(config)#int tunnel 0
Corp(config-if)#tunnel mode gre ip
Corp(config-if)#ip address 192.168.10.1 255.255.255.0
Corp(config-if)#tunnel source 63.1.1.1
Corp(config-if)# tun destination 63.1.1.2
```

```
SF(config)#int s1/0
SF(config-if)#ip address 63.1.1.2 255.255.255.252
SF(config-if)#int tunnel 0
SF(config-if)#ip address 192.168.10.2 255.255.255.0
SF(config-if)#tunnel source 63.1.1.2
SF(config-if)#tun destination 63.1.1.1
```

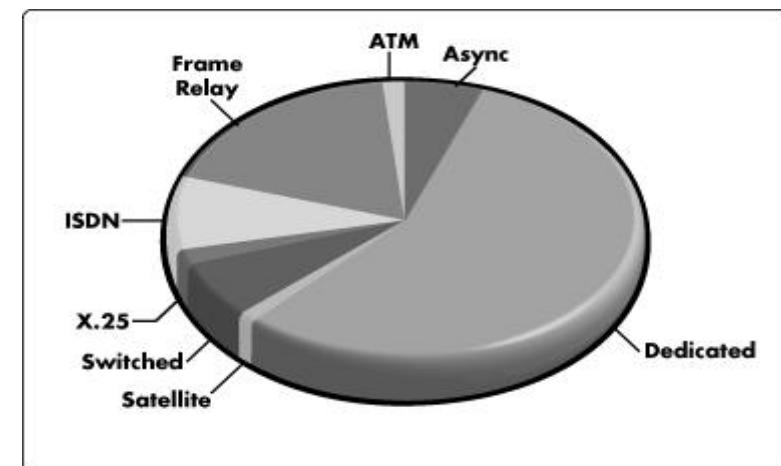
To Verify:

```
Corp#sho run
Corp#sh ip int brief
Corp#sh int tun 0
Corp#sh ip route
Corp#ping 192.168.10.2
```



WAN Technologies

eBGP



What Is BGP?

- Border Gateway Protocol Version 4
- Standards based
 - RFC 4271 “A Border Gateway Protocol 4 (BGP-4)”
- Exterior Gateway Protocol (EGP)
 - Used for inter-domain routing between Autonomous Systems
- Path vector routing
 - Uses multiple “attributes” for routing decision
- Classless
 - Supports VLSM and summarization

Inter-AS Routing and ASNs

- Autonomous System (AS)
 - "...a set of routers under a single technical administration, using an interior gateway protocol (IGP) and common metrics to determine how to route packets within the AS, and using an inter-AS routing protocol to determine how to route packets to other ASes." (RFC 4271)
- Like IP address space, Autonomous System Numbers (ASNs) allocated by Internet Assigned Numbers Authority (IANA)
 - <http://www.iana.org/numbers/>
- BGP ASNs originally 2-byte field
 - Values 0-65535
- RFC 4893 defines 4-byte ASNs
 - 0.0 – 65535.65535 notation
 - 0.[0-65535] denote original 2-byte ASNs

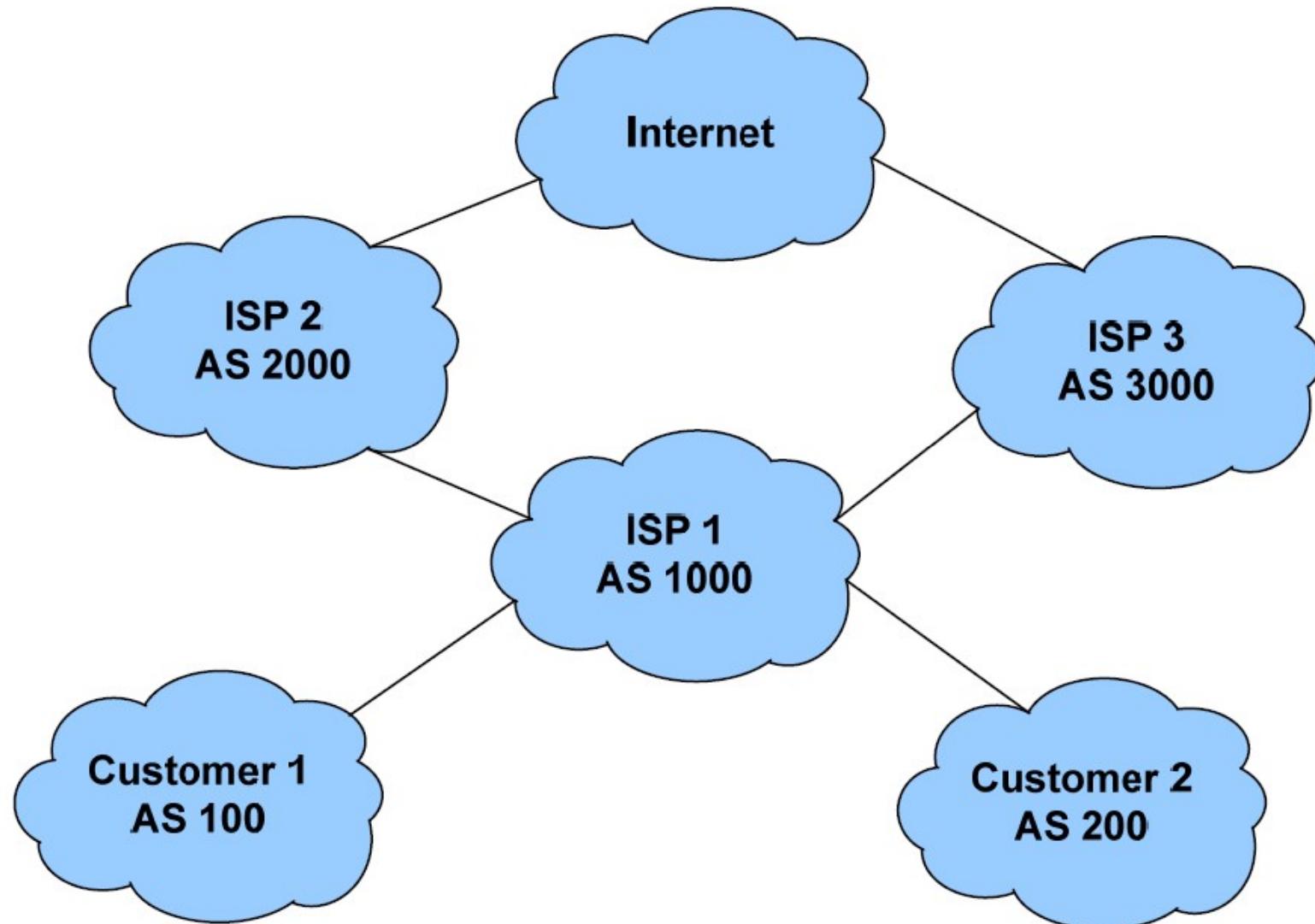
Why Use BGP?

- Scalability
 - IGPs can scale to thousands of routes
 - BGP can scale to hundreds of thousands of routes
 - Current Global (Internet) BGP table ~ 300,000 routes
- Stability
 - Internet routing table *never converges*
 - BGP stable enough to handle routing and decision making at the same time
- Enforce routing policy
 - IGP uses link cost for routing decision
- Effective traffic engineering nearly impossible with IGP
 - BGP uses attributes of the route itself
- Traffic engineering feasible and simple to implement

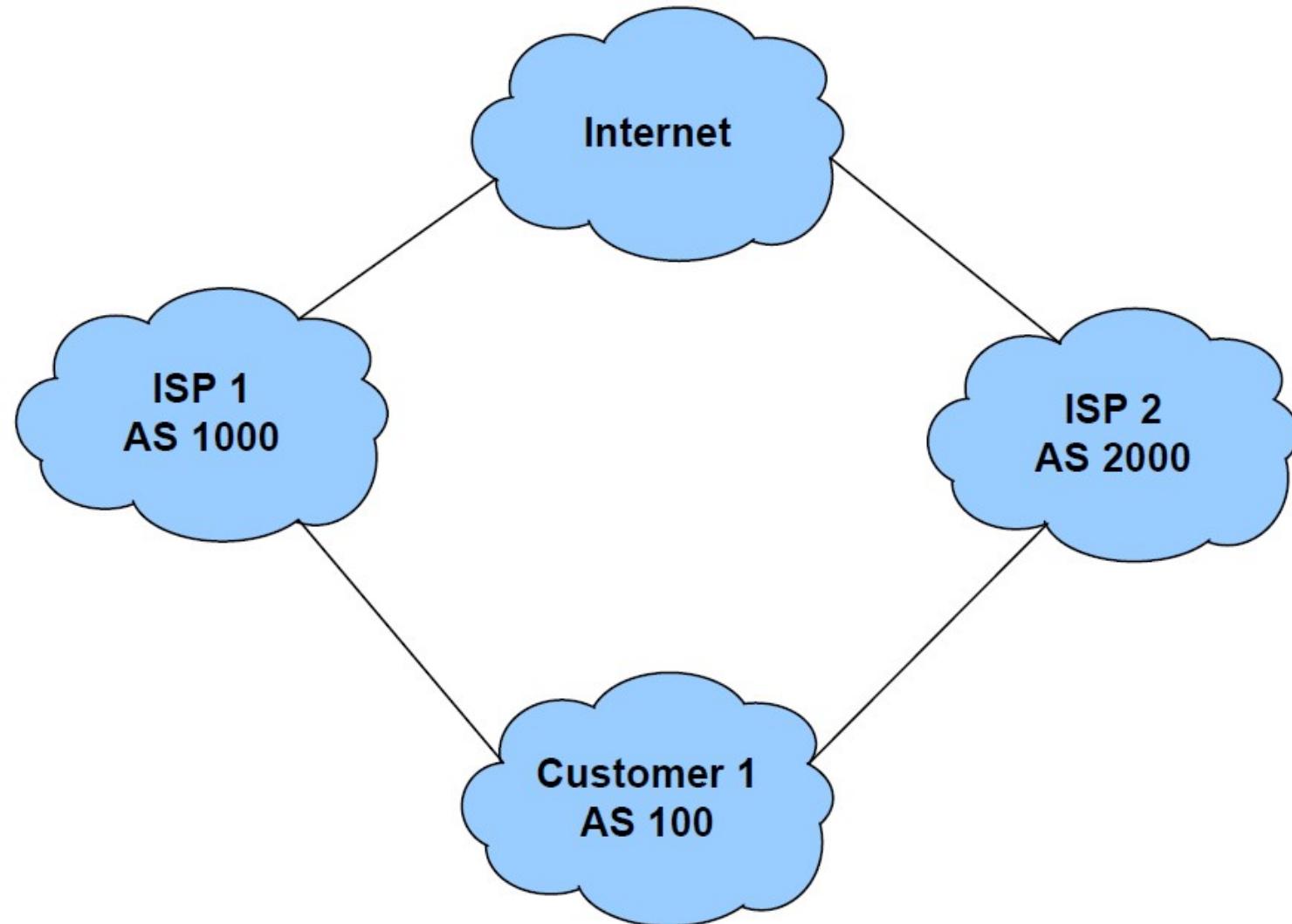
Who Needs BGP?

- Transit networks
 - SPs that sell access or transit bandwidth to customers
 - Need full routing table to make accurate decisions
 - Should not use default routing
- Multihomed networks
 - Enterprise networks with two or more connections to ISPs
 - Allows control

Example Transit Network



Example Multihomed Network



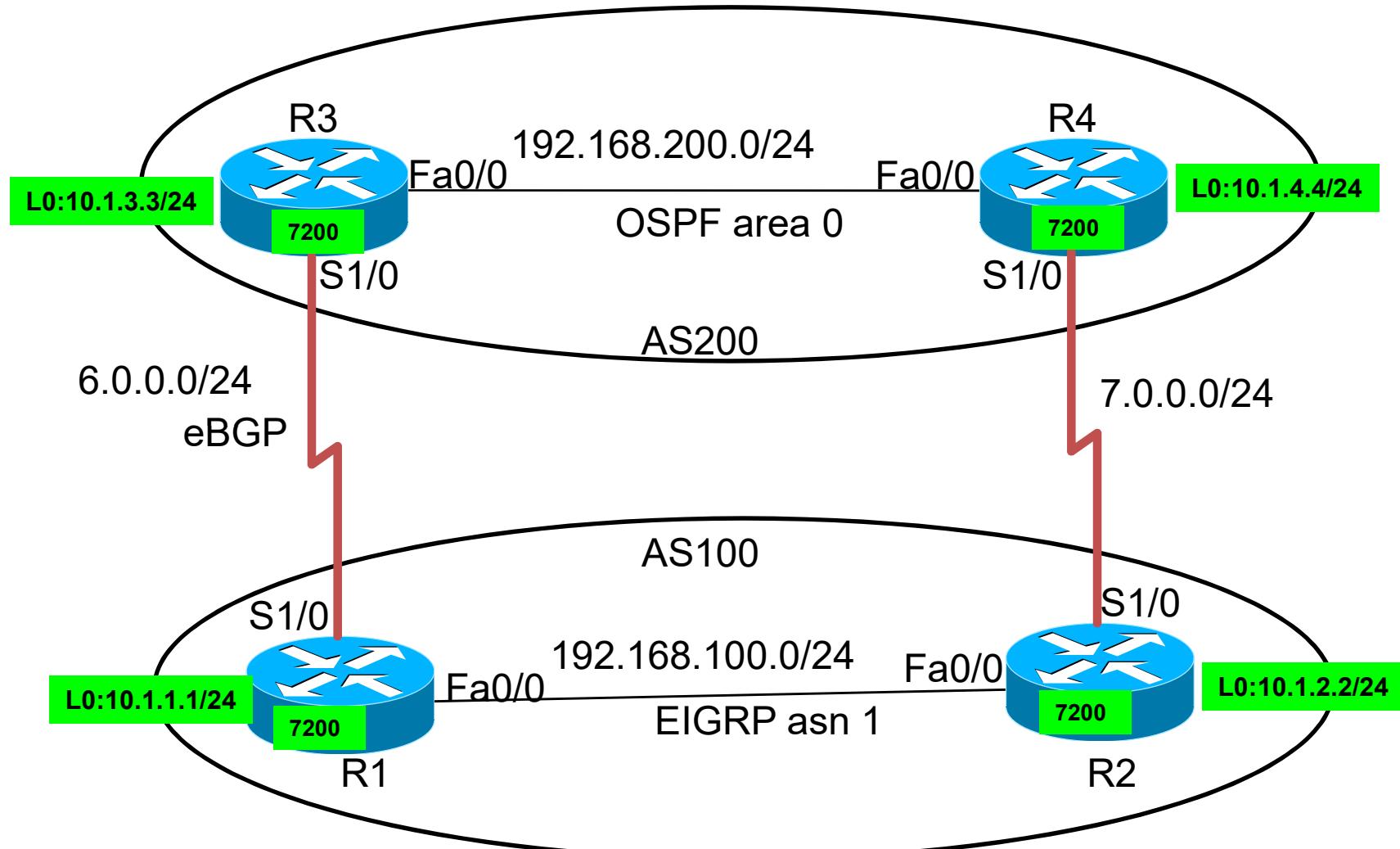
When not To Use BGP

- Single ISP connectivity
 - Default routing sufficient
- Limited memory and/or CPU resources
 - Global table needs ~ 1GB of memory just for storage
- If you don't "own" your IPv4 addresses
 - ISP advertises "their" address space on your behalf
 - Red tape involved with getting IP address space and BGP ASN

Basic BGP Configuration

- Enable global BGP process
 - **router bgp [ASN]**
- Establish BGP peers
 - **neighbor [address] remote-as [remote ASN]**

eBGP Topology



IP Addressing Schema: X.X.X.hostname

Basic BGP Peering Configuration

Peering

```
R1#
router bgp 100
neighbor 6.0.0.3 remote-as 200
```

```
R2#
router bgp 100
neighbor 7.0.0.4 remote-as 200
```

```
R3#
router bgp 200
neighbor 6.0.0.1 remote-as 100
```

```
R4#
router bgp 200
neighbor 7.0.0.2 remote-as 100
```

Route advertisement

```
R1#
router bgp 100
network 192.168.100.0 mask 255.255.255.0
network 10.1.1.0 mask 255.255.255.0
network 6.0.0.0 mask 255.255.255.0
```

```
R2#
router bgp 100
network 192.168.100.0 mask 255.255.255.0
network 10.1.2.0 mask 255.255.255.0
network 7.0.0.0 mask 255.255.255.0
```

```
R3#
router bgp 200
network 192.168.200.0 mask 255.255.255.0
network 10.1.3.0 mask 255.255.255.0
network 6.0.0.0 mask 255.255.255.0
```

```
R4#
router bgp 200
network 192.168.200.0 mask 255.255.255.0
network 10.1.4.0 mask 255.255.255.0
network 7.0.0.0 mask 255.255.255.0
```



Basic BGP Verification

- Verify BGP peerings
 - **show ip bgp summary**
- Verify BGP table
 - **show ip bgp**
- Verify BGP table detail
 - **show ip bgp [network] [mask]**
- Verify BGP routing table
 - **show ip route [bgp]**

Telnet: **route-views.oregon-ix.net**



Infrastructure Security

Terminologies

Lesson 41



Security Terminologies

1. Asset
 - Anything value for organization i.e. People, Property, Information(IT)
2. Vulnerability
 - Weakness – OS, Router, Switch
3. Intrusion/Attack/Exploit
 - Hacker/Terrorist/Unsatisfied Users
4. Threat [Security Audit - VA/PT]
 - On-going Attack on Asset's vulnerability
5. Risk (Impact & Priority)
 - Assessment – Low, Medium & High
6. Countermeasure
 1. For high risks :
 - **Administrative:** Good Security Policy
 - **Technical:** AAA, FW, IPS, ACL, Anti-virus, 802.1x
 - **Physical :** CCTV, UPS & ACS
7. Mitigation
 1. Implementing countermeasures
 - Stop/Reduce/Awareness [Trainings, workshop, drills]



Infrastructure Security

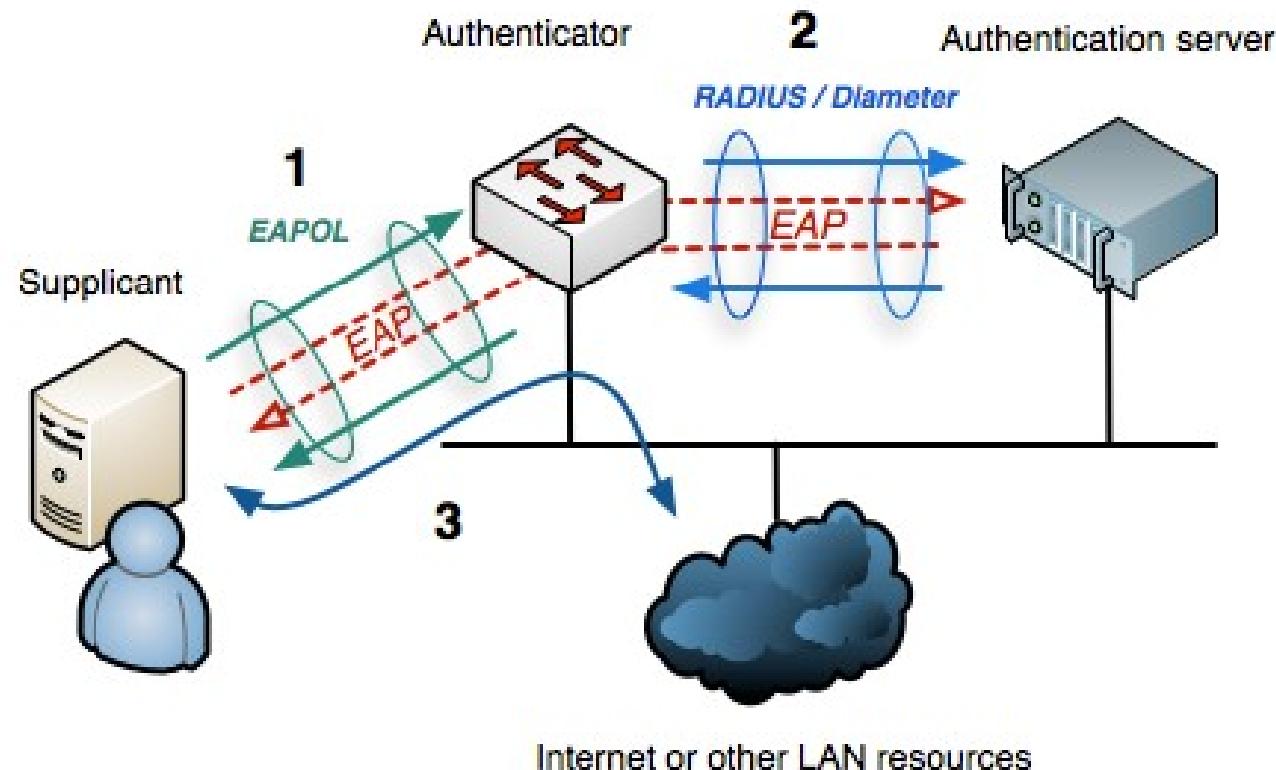
Access layer threat mitigation Techniques

Lesson 41

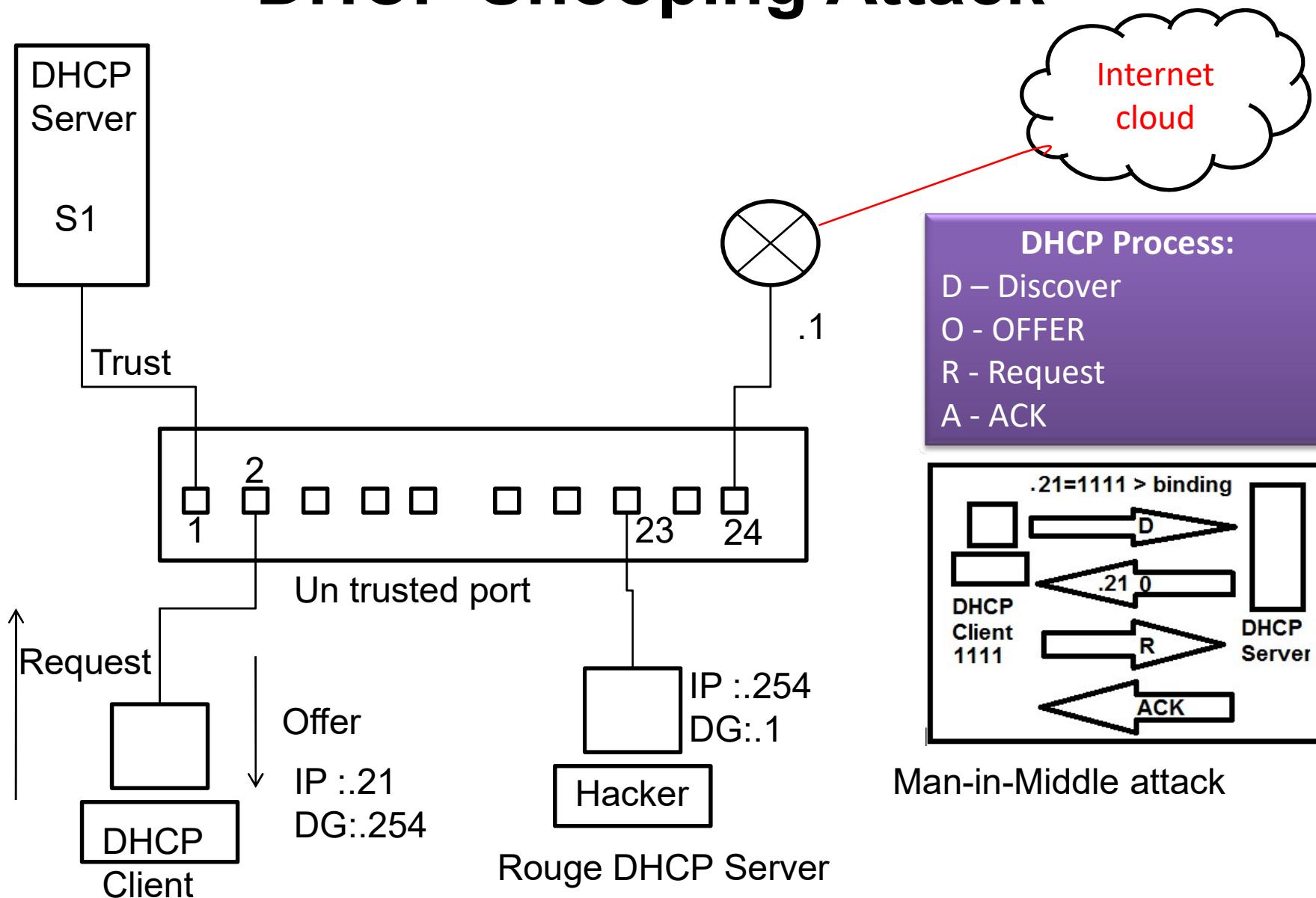


802.1x

- IEEE **802.1X** is an IEEE Standard for port-based Network Access Control (PNAC)



DHCP Snooping Attack



DHCP Snooping Commands

To configure

- **Switch(config)# ip dhcp snooping**
- **Switch(config)# ip dhcp snooping vlan 1**
- **Switch(config-if)# interface fa 0/1**
- **Switch(config-if)# ip dhcp snooping trust**

To Verify:

- **Switch# show ip dhcp snooping**



Nondefault native VLAN

1. Native VLAN

1. By default - All interface native vlan 1
2. Create Rest vlan i.e. VLAN 200
3. Assign all interfaces to vlan 200
4. Configure native vlan command for vlan 200

Commands:

- interface FastEthernet0/1
- switchport access vlan 200
- switchport trunk native vlan 200
- switchport trunk encapsulation dot1q
- switchport mode trunk



Infrastructure Security

APIC-EM path trace ACL analysis tool

Lesson 41



APIC-EM path trace ACL analysis tool

1. Application Policy Infrastructure Controller – Enterprise Module
 1. Software-Defined Networking (SDN) controller for enterprise networks (in the campus or branch and the WAN)
 2. Troubleshooting ACL & WAN related problems
2. Check in my you-tube channel
 1. kumar6009@gmail.com or kumar



Infrastructure Security

Basic device hardening

Lesson 41



Basic Device hardening

- Local authentication
 - Username & Password
 - Login Local
- Secure password
 - Encrypted
 - Enable secret & service password-encryption
- Access to device
 - Source address
 - Telnet/SSH
- Login banner

Infrastructure Security

Device security using AAA {TACACS+ & RADIUS}

Lesson 41



Terminologies

1. Cisco Secure ACS, RADIUS, and TACACS
 - Cisco ACS, Platform, ISE, Protocols, Appillance
2. AAA – Centralized User Management
 1. Authentication – Who can access?
 2. Authorization – What can be accessed?
 3. Accounting – What you do? (logs/auditing)
3. AAA Protocols
 1. TACACS+ - Cisco Proprietary
 2. RADIUS – Open Standard Protocol
4. AAA Method List –
 1. Order of authentication- 1.Tacacs+, Local, Enable, None

Cisco Secure ACS, RADIUS, and TACACS

	TACACS+	RADIUS
Functionality	Separates AAA functions into distinct elements. Authentication is separate from authorization, and both of those are separate from accounting.	Combines many of the functions of authentication and authorization together. Has detailed accounting capability when accounting is configured for use.
Standard	Cisco proprietary, but very well known.	Open standard, and supported by nearly all vendors' AAA implementation.
L4 protocol	TCP.	UDP.
Confidentiality	<i>All</i> packets are encrypted between the ACS server and the router (which is the client).	Only the password is encrypted with regard to packets sent back and forth between the ACS server and the router.
Granular command by command authorization	This is supported, and the rules are defined on the ACS server about which commands are allowed or disallowed.	No explicit command authorization checking rules can be implemented.
Accounting	Provides accounting support.	Provide accounting support, and generally acknowledged as providing more detailed or extensive accounting capability than TACACS+.

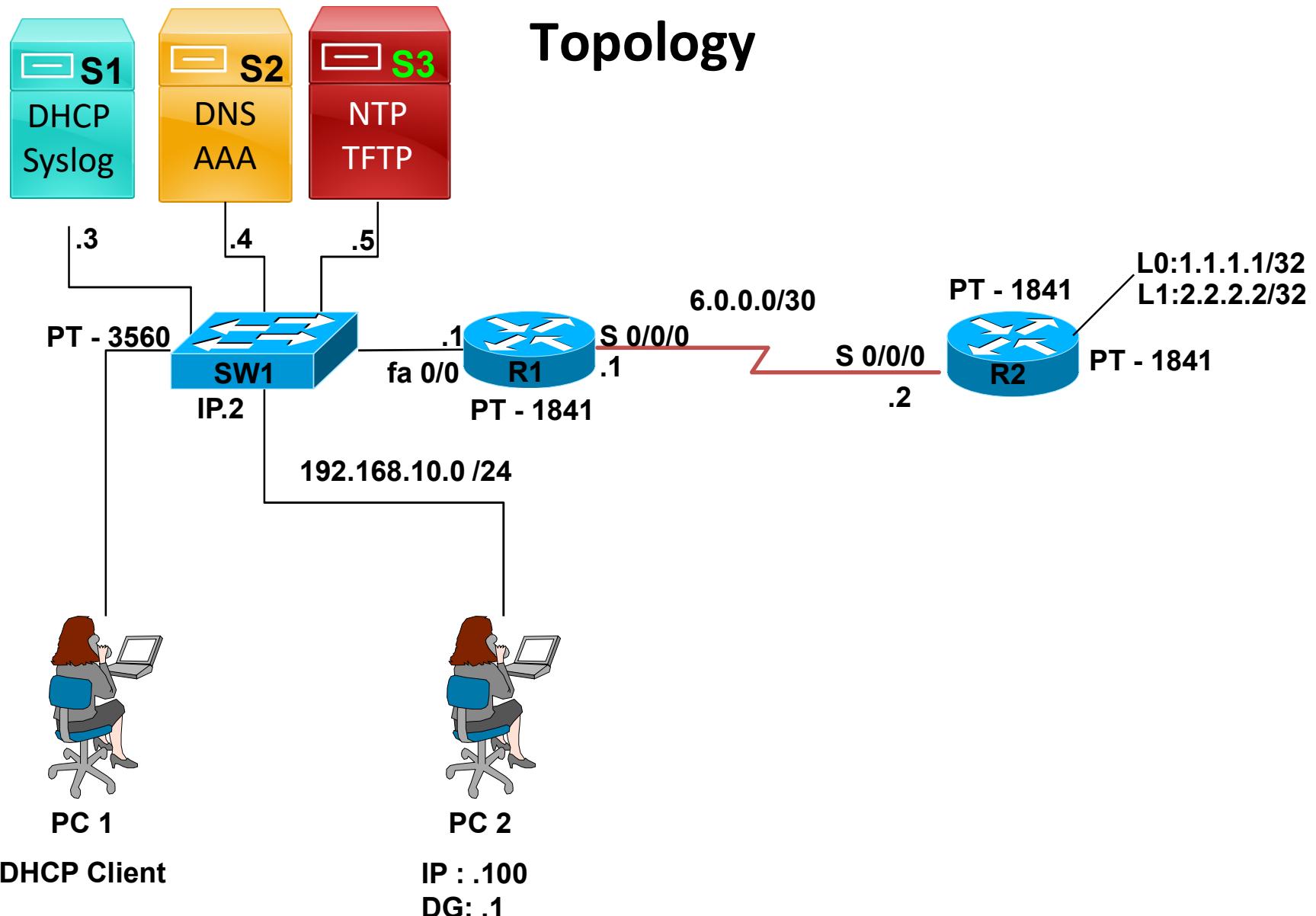


Configure, Verifying & Troubleshooting Concepts

Task	How to Do It
Decide what the policy should be (for example, which vty lines should require authentication/authorization) and which methods (ACS, local, none) should be used.	This step is done way before you ever begin configuring the router, and is based on your security policy for your network. It is the concept of what you want to accomplish for authentication and authorization.
Enable the ability to configure AAA.	<code>aaa new-model</code> is not enabled by default. If you want to use the services of ACS, you must enable the feature of AAA as the very first step of configuration on a new router.
Specify the address of an ACS server to use.	Use the <code>tacacs-server host</code> command, including the IP address of the ACS server and the password.
Create a named method list for authentication and another for authorization, based on your policy.	Each method list is created in global configuration mode, specifying which methods this list uses, in order, from left to right.
Apply the method lists to the location that should use those methods.	In vty line configuration mode, specify the authentication and authorization method lists that you created in the preceding step.



Configure, Verifying & Troubleshooting Topology



Configure, Verifying & Troubleshooting

• **Configure: Commands**

- R1(config)# username admin password cisco
- R1(config)# aaa new-model
- R1(config)# tacacs-server host 192.168.10.4 key cisco
- R1(config)# aaa authentication login default group tacacs+ local
- R1(config)# do ping 192.168.10.4
- R1(config)# line vty 0 15
- R1(config-line)# login authentication default

• **To Verify:**

- R1# debug aaa authentication
- R1# telnet 192.168.10.1

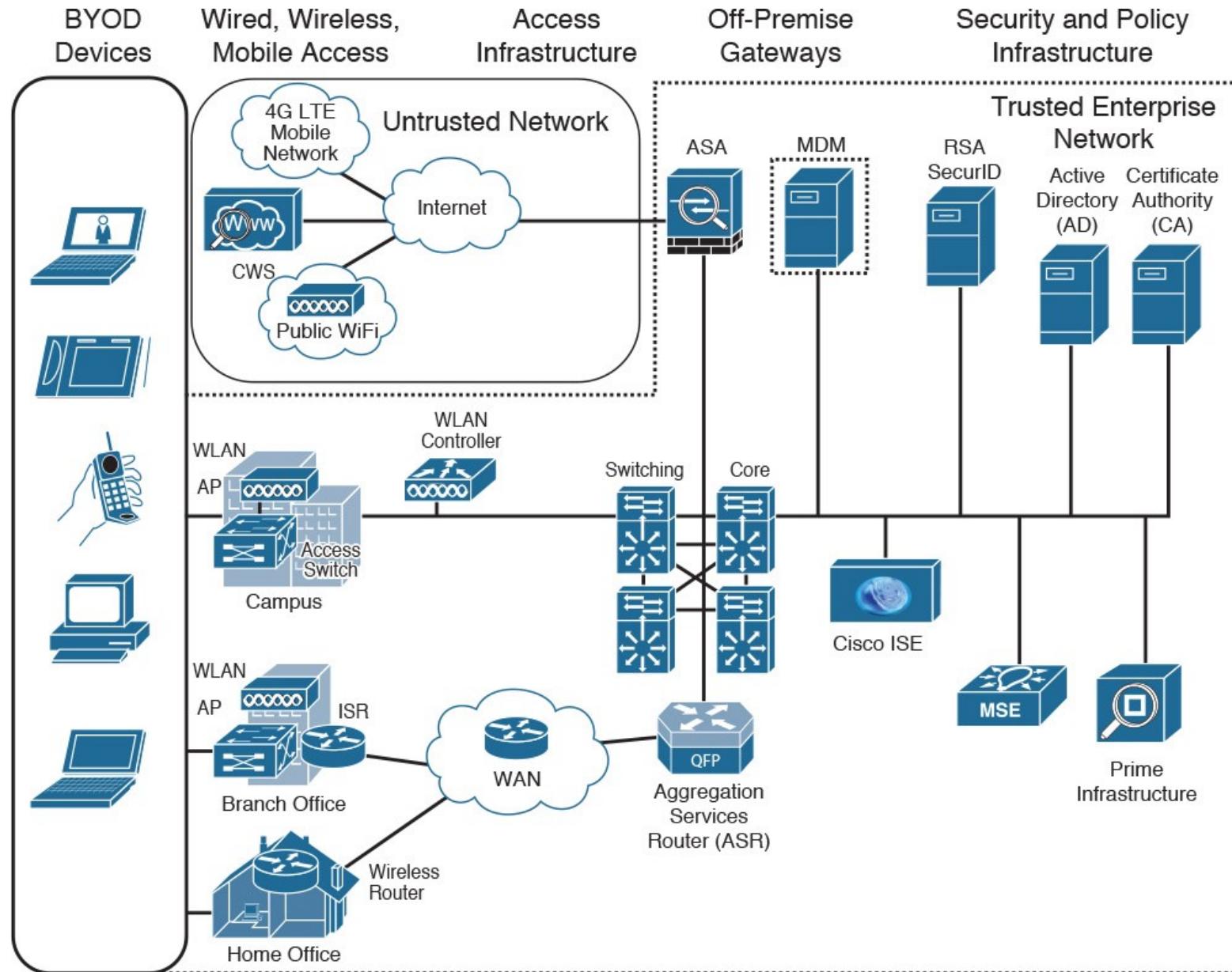
Infrastructure Security

Switch Port Security

Lesson 41



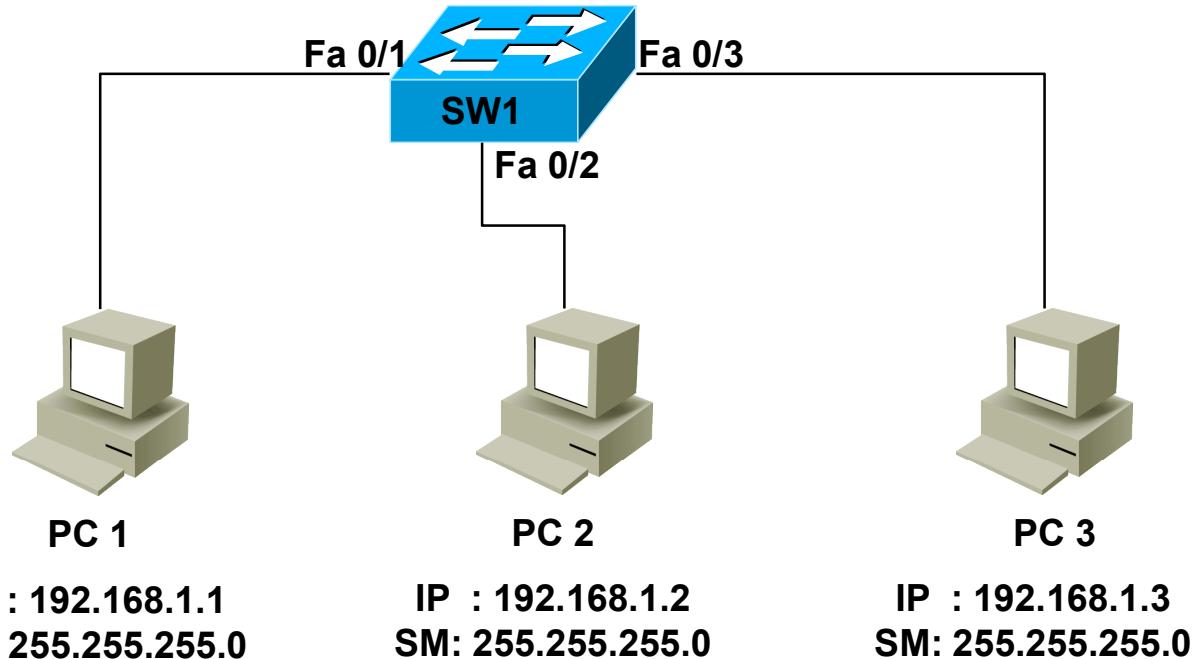
BYOD Architecture



Switch Port Security - Concepts

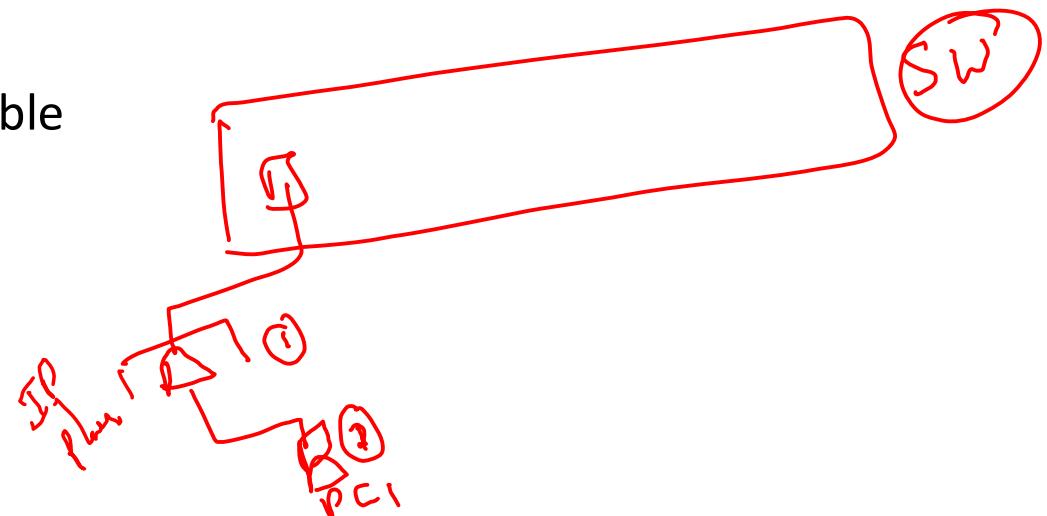
- Why we care what plugs into our network?
 - BYOD Architecture
- Port security Allows you to restrict connections to the LAN in two ways
 - Number of MAC address per port
 - What MAC address is on a port
- Violation modes
 - Shutdown –Default – Error-disable
 - Protect – No reaction & No log
 - Restrict – Send sys log message

Switch port security – Topology



Switch port security - Commands

- SW1(config)# int fa0/1
- SW1(config-if)# switchport port-security
 - {Activation command - last}
- SW1(config-if)# switchport mode ~~access~~
2- voice
- SW1(config-if)# switchport port-security maximum 1
data
- SW1(config-if)# switchport port-security violation restrict
- SW1(config-if)# switchport port-security mac-address sticky
- To verify:
 - SW1#show mac-address table



Infrastructure Management

Device-monitoring protocols

SNMP



SNMP - Concepts

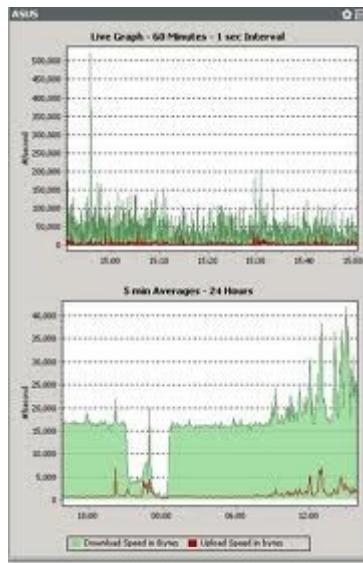
- Simple Network Management Protocol
- SNMP “simply” grabs statistics from devices
- Monitoring Applications manipulate & convert the raw data {excel sheet} to graphical format i.e. Graph, Pie chart
- OID – Object Identifier
 - 1.1.1.1.62.69.55.1.1.1.68.....line protocol
 - Library
 - MIB – Meta Information Base
 - Import MiB to Management Console

SNMP - Concepts

- Monitoring Applications
 - Free
 - MRTG
 - PRTG
 - Solar winds
 - HP Open view i.e. Global Certifications
 - Cisco Prime Infrastructure
 - IBM Trivoli
- Three versions
 - V1
 - old & not used
 - V2 (Recommended)
 - Popular & simple
 - Little security i.e. Community string {Default: Public} + R0/RW
 - V3 (Security)
 - User Name, Password, Encryption & Group

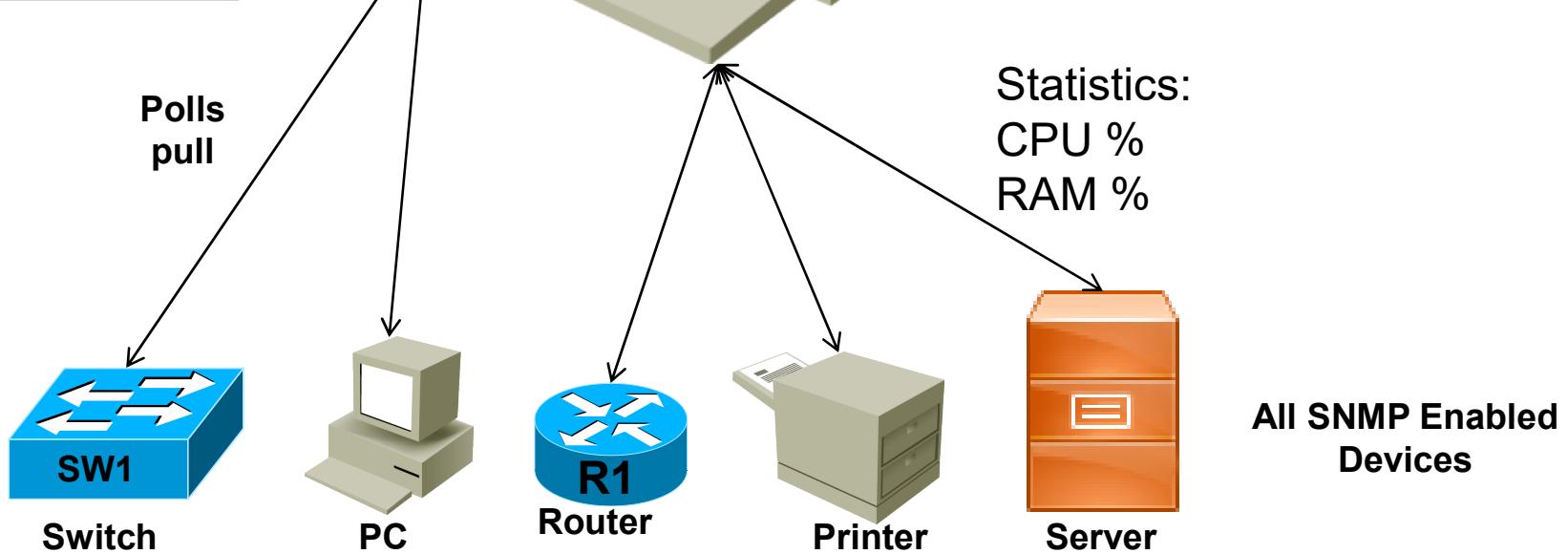
SNMP - Topology

RAW Data → Graph



SNMP Management Console

i.e. MRTG/PRTG
HP – Open view
Cisco prime Infrastructure



SNMP - Commands

- SNMPv2 Syntax
 - R1 (config)# snmp server community [string] [ro/rw]
- Command:
 - R1 (config)# snmp-server community cisco ro
- To verify:
 - R1#show snmp community

SNMPv3:

! Enter global configuration mode

CCNA-Router# **configure terminal**

! Configure the community string along with an access-list to restrict access

CCNA-Router(config)# **snmp-server community CCNA RO 99**

! Create the IP Standard Access List defined in the previous step

CCNA-Router(config)# **access-list 99 permit 192.168.1.0 /24**

! Configure the v3 for no authentication (noauth)

CCNA-Router(config)# **snmp-server group CCNA-group v3 noauth**

! Configure a v3 user that resides in the v3 group

CCNA-Router(config)# **snmp-server user CCNA-user CCNA-group v3**

! Configure the community string and access-list to restrict SNMP to hosts in the

! 192.168.1.0/24 subnet

CCNA-Router(config)# **snmp-server community CCNA RO 99**

! Specify interface to be used for SNMP traps

CCNA-Router(config)# **snmp-server trap-source FastEthernet0/1**

! Specify the SNMP v3 server that will be allowed SNMP access

CCNA-Router(config)# **snmp-server host 192.168.1.96 version 3 noauth CCNA-user**



Infrastructure Management

Device-monitoring protocols

SYSLOG



Syslog

- Capturing Syslog :
 - Syslog captures key status messages from cisco devices
 - Each device can store syslog messages locally or on a remote server
 - Syslog uses UDP port 514
- Monitoring Applications:
 - Kiwi syslog server {solar winds}
 - Splunk
- Commands:
 - Logging “Host name or A.B.C.D”
 - R1(config)#logging 192.168.1.2



Syslog Levels & Output



Level	Keyword	Description	Definition
0	emergencies	System is unusable	LOG_EMERG
1	alerts	Immediate action is needed	LOG_ALERT
2	critical	Critical conditions exist	LOG_CRIT
3	errors	Error conditions exist	LOG_ERR
4	warnings	Warning conditions exist	LOG_WARNING
5	notification	Normal but significant condition	LOG_NOTICE
6	informational	Informational messages only	LOG_INFO
7	debugging	Debugging messages	LOG_DEBUG

Syslog Server					
File Edit View Help					
Display 00 (Default) ▾					
!	Date	Time	Priority	Hostname	Message
09-27-2012	13:29:10	Cron.Alert	208.132.97.91	Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test	
09-27-2012	13:29:10	Local0.Critical	215.57.221.47	Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test	
09-27-2012	13:29:10	System3.Debug	222.96.144.194	Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test	
09-27-2012	13:29:10	Local5.Critical	199.148.120.158	Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test	
09-27-2012	13:29:10	Local6.Alert	212.225.146.101	Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test	
09-27-2012	13:29:10	System4.Alert	212.80.189.160	Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test	
09-27-2012	13:29:10	System2.Warning	224.82.223.225	Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test	
09-27-2012	13:29:10	System4 Notice	211.118.97.185	Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test	
09-27-2012	13:29:10	Local1.Warning	209.202.119.89	Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test	
09-27-2012	13:29:10	Lpr Notice	220.201.229.221	Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test	
09-27-2012	13:29:10	Local5.Error	221.211.21.154	Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test	
09-27-2012	13:29:10	Local1 Notice	197.122.152.202	Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test	
09-27-2012	13:29:10	Local6.Alert	205.47.191.161	Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test	
09-27-2012	13:29:10	Mail.Info	221.19.157.147	Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test	
09-27-2012	13:29:10	Daemon.Error	208.238.142.66	Sep 27 13:29:10 BJS-003-Win2003 SyslogGen This is Syslog test	



Infrastructure Management

ICMP echo-based IP SLA



ICMP based IP SLA - Concepts

0. Topology
1. Host Name
2. Ip address
3. Serial
4. Routing protocol – eigrp
5. Ping R1 ->S1
6. ICMP based IPSLA
 1. Ping s1 for every 60 sec forever
7. Verify

ICMP Based IP SLA – Topology

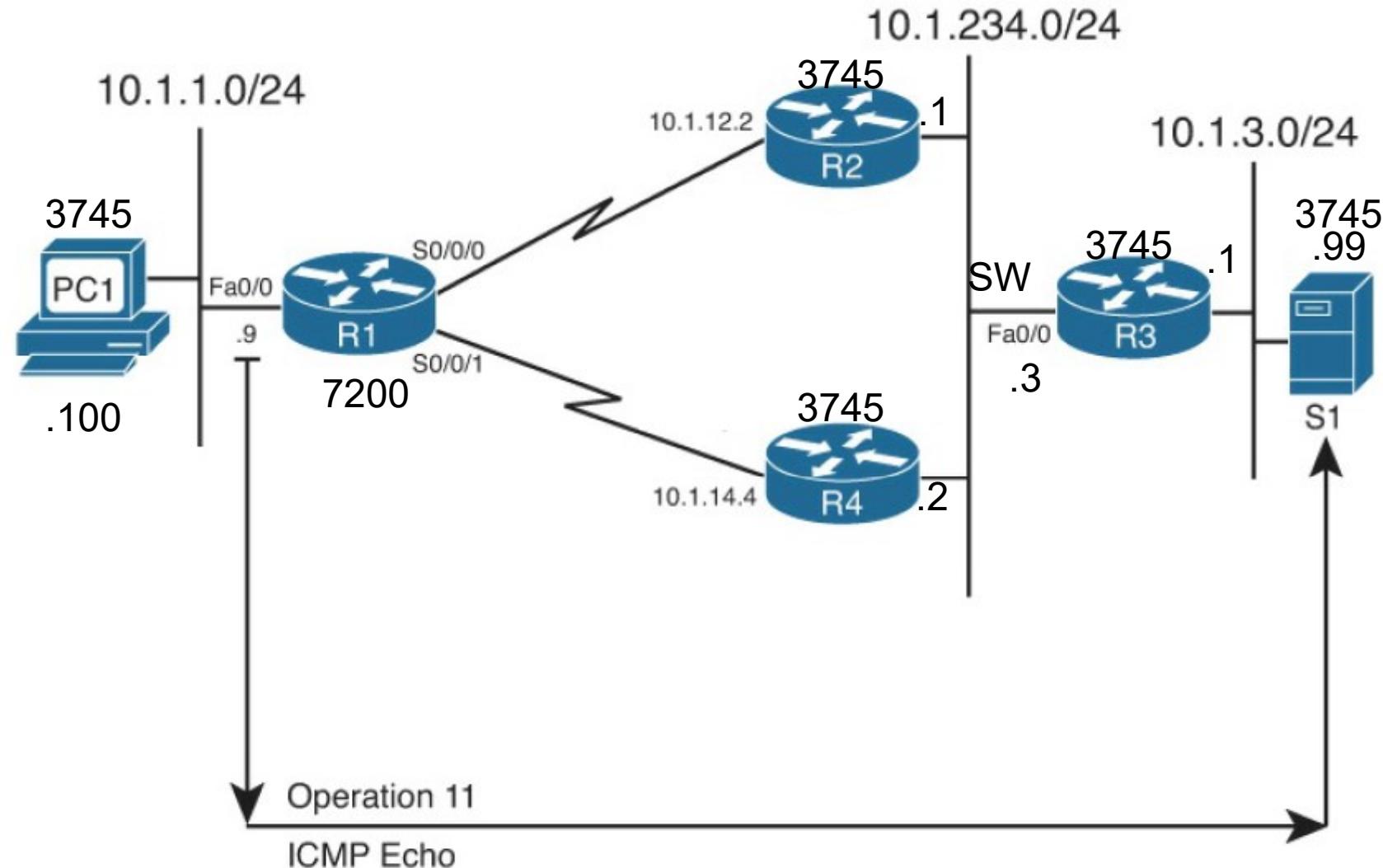


Figure 11-8 Concept of IP SLA Operation on R1

ICMP Based IP SLA - Commands

- R1# **conf t**
- Enter configuration commands, one per line. End with CNTL/Z.
- R1(config)# **ip sla 11**
- R1(config-ip-sla)# **icmp?**
- icmp-echo icmp-jitter
- R1(config-ip-sla)# **icmp-echo 10.1.3.1 source-ip 10.1.1.1**
- R1(config-ip-sla)# **frequency 60**
- R1(config-ip-sla)# **exit**
- R1(config)# **ip sla schedule 11 start-time now life forever**
verify:
 - R1# **show ip sla configuration**
 - R1# **show ip sla statistics 11**

Infrastructure Management

Device Management



Table of Contents

- TFTP - Backup and restore device configuration
- Using Cisco Discovery Protocol or LLDP for device discovery
- Logging i.e. syslog
- Time zone
- Loopback
- Licensing

- Before IOS version15 (12.x versions and prior)
 - No Licensing
 - Different IOS for different services
 - IP Base (12.1) - ADV. Security (12.4T) - ADV. IP services (12.4 [15]T1)
 - IP voice - ENT. Base -ENT Services
 - After IOS version15
 - Licensing
 - Universal IOS with all feature inclusive, services will be activated with license keys
 - IP Base - Permanent
 - Data {MPLS, ATM, Multi-protocol} - Not Activated
 - Unified Communication - Not Activated
 - Security {Firewall, VPN, & Encryption} - Evaluation

IOS Licensing - Commands



12.4(15)T1



15.1(4)M4

- To verify:
 - R1# show version

- Command:
 - R1 (config)# “License” command
 - R1 (config)# “License-Install” command

Infrastructure Management

Initial Device Configuration



Initial Device configuration

- Routing
 - Hostname
 - Interface fa0/0 - IP address
 - Console, enable, vty password (telnet/SSH)
 - SNMP/syslog/banner config
- Switching
 - Hostname
 - MGT Interface (VLAN 1) - IP address
 - Console, enable, vty password (telnet/SSH)
 - SNMP/syslog/banner config

Infrastructure Management

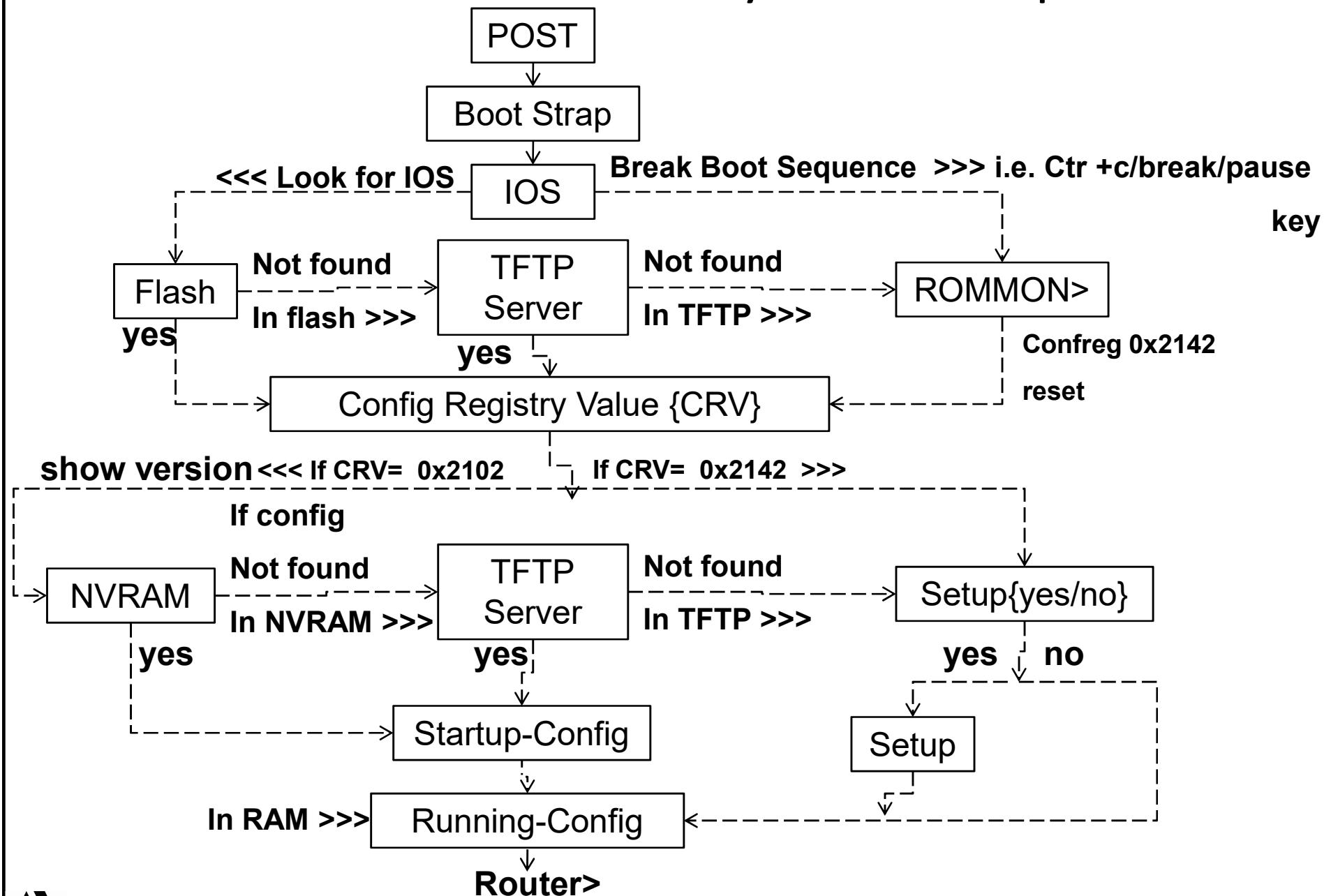
Device maintenance



Table of Contents

- Cisco IOS upgrades and recovery
 - SCP, FTP, TFTP, and MD5 verify
 - SCP - Secure Copy Protocol
 - provides a secure and authenticated method for copying device configurations or device image files
 - SCP Configuration
 - CCNA-Router# configure terminal
 - Enter configuration commands, one per line. End with CNTL/Z.
 - CCNA-Router(config)# ip scp server enable
 - CCNA-Router(config)# exit
 - FTP - File Transfer Protocol (TCP-ACK)
 - TFTP - Trivial File Transfer Protocol (UDP – No ACK)
 - MD5 – Message Digest version 5
 - Algorithm that is used to verify **data integrity (data should change only by authorised user)** through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual.
 - » <http://crypto.hurlant.com/demo/>





Router Password Recovery - Commands

- To break the IOS boot Process:
 - Ctrl + C/Pause/Break
- ROMMON>
 - ROMMON> confreg 0x2142
 - ROMMON> reset
- IOS Command:
 - R1 (config)# config-register 0x2102
 - R1 # reload
- To Verify:
 - R1 # show version



File system management

- [cd](#)
- [cfs check](#) - Configuration File System
- [copy](#)
- [delete](#)
- [dir](#)
- [erase nvram:](#)
- [erase nvram-raw:](#)
- [Format](#)
- [fsck](#) - To check a file system for damage
- [mkdir](#)
- [pwd](#)
- [rmdir](#)
- [show filesystem](#)
- [show media](#)
- [unmount](#)

For more details:

http://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-2/system_management/command_reference/b_sysman_cr42asr9k/b_sysman_cr42asr9k_chapter_0111.html



Infrastructure Management

IOS tools



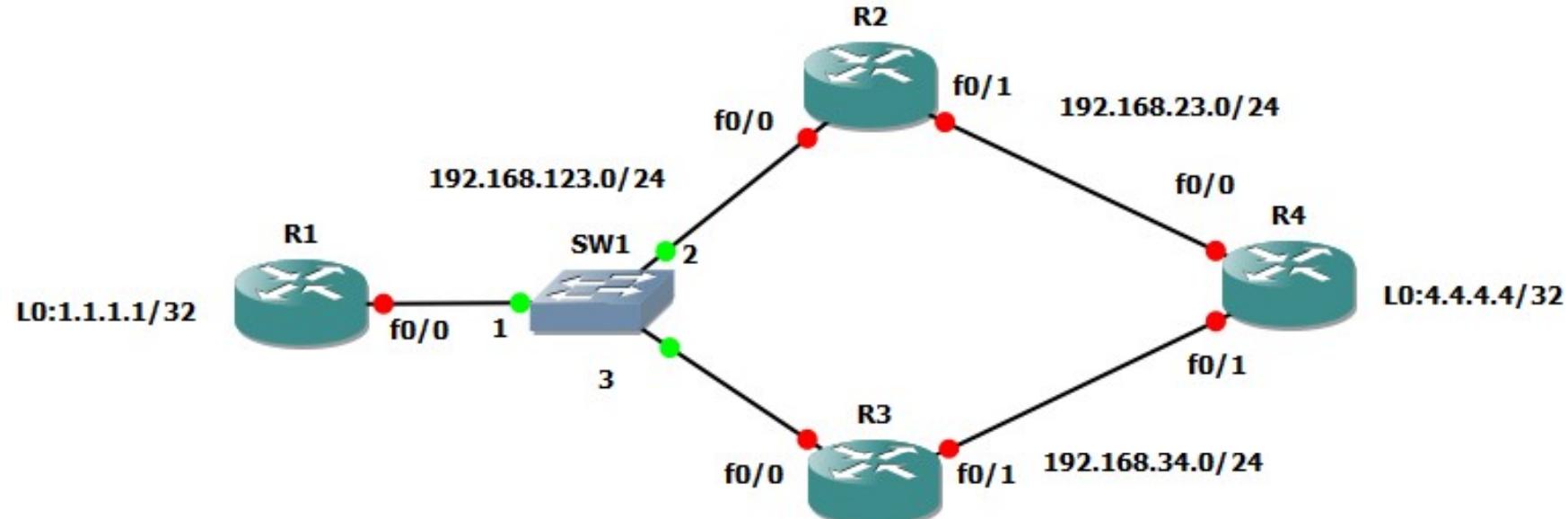
Table of Contents

- Ping and traceroute with extended option
- Terminal monitor
 - CISCO IOS doesn't send log messages to a terminal session over IP(i.e telnet or SSH connections).If you want logging messages from IOS to appear on the terminal, use terminal monitor command.
- Log events
- Local SPAN
 - Switch Port Analyzer

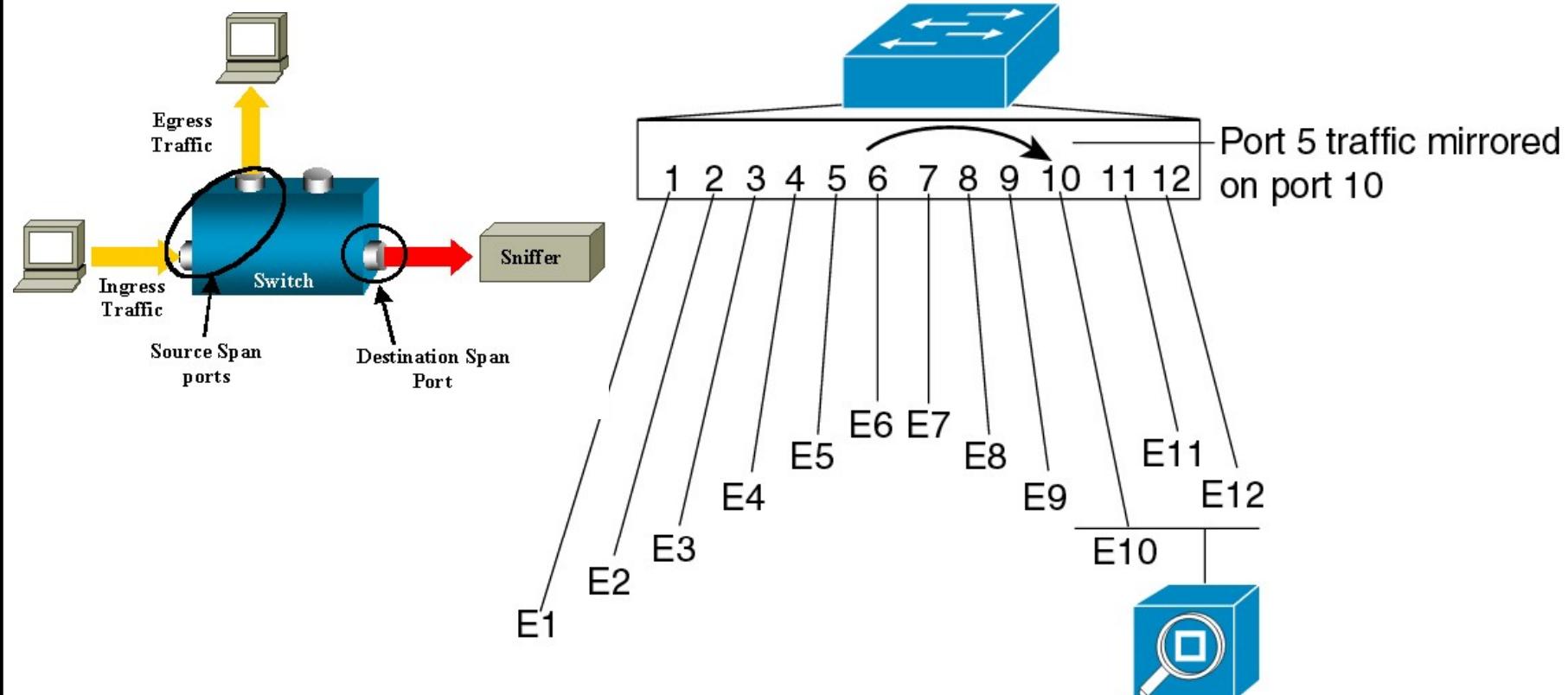


Ping and Traceroute – Lab - Topology

IP addressing schema: 192.168.hosts-name.hostname



Local SPAN



Fast Ethernet port 0/6 as a bidirectional source for session 1:

```
SW1(config)# monitor session 1 source interface fastethernet 0/6
```

Fast Ethernet port 5/48 as the destination for SPAN session 1:

```
SW1(config)# monitor session 1 destination interface fastethernet 0/10
```

To disable SPAN:

```
SW1(config)# no monitor session [session no]
```



Infrastructure Management

Network Programmability



Networking Software Systems

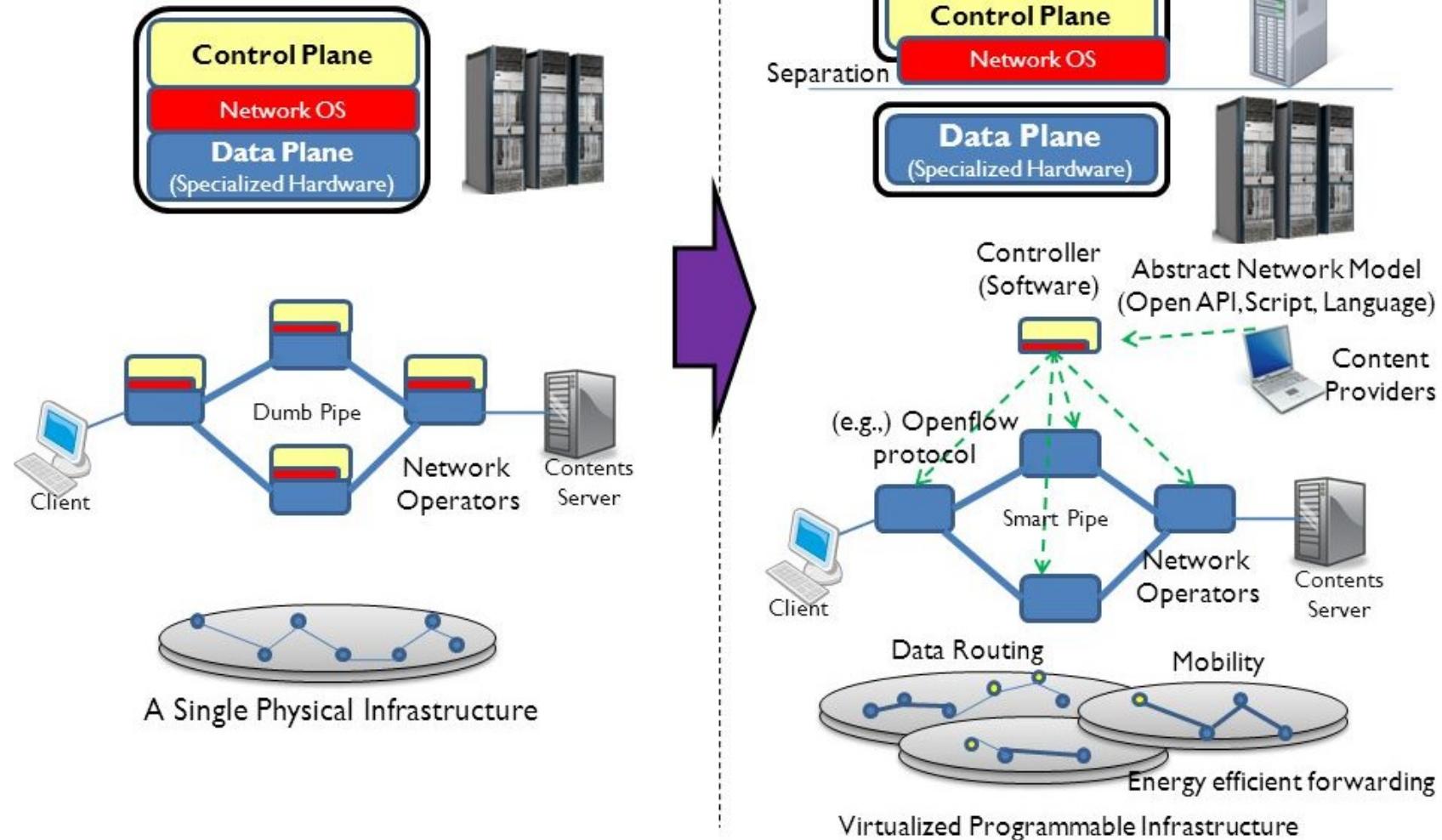
- **IOS**
 - Integrates technology, business services, and hardware support
 - Reduces operational spending
 - Optimizes return on investment
 - Improves business productivity
- **IOS XE**
 - Supports next-generation platforms
 - Runs as a single daemon within a modern Linux operating system
 - Separates the data plane and control plane
 - Improved services integration
- **IOS XR**
 - Focuses on the needs of service providers
 - Designed for the dynamic network usage requirements of services
 - Flexible programmability for dynamic reconfiguration
- **NX-OS**
 - Open, modular and programmable for an agile data center infrastructure
 - Optimized for both physical and virtual data center deployments
 - Highly reliable continuous system operation, optimizing uptime

Terminologies

- Evolution of Intelligent Network i.e. AI – Artificial Intelligence
 - Make Machine Intelligent i.e. Thinking, self –knowledge up-gradation & Decision-making
 - Inspection, interrogation, and remediation of network problems
- Function of a controller
 - An **SDN controller** is an application in **software-defined networking (SDN)** that manages flow **control** to enable intelligent networking. **SDN controllers** are based on protocols, such as OpenFlow, that allow servers to tell switches where to send packets.
- API
 - Application program interface (**API**) is a set of routines, protocols, and tools for building software applications. An **API** specifies how software components should interact and **APIs** are used when programming graphical user interface (GUI) components.

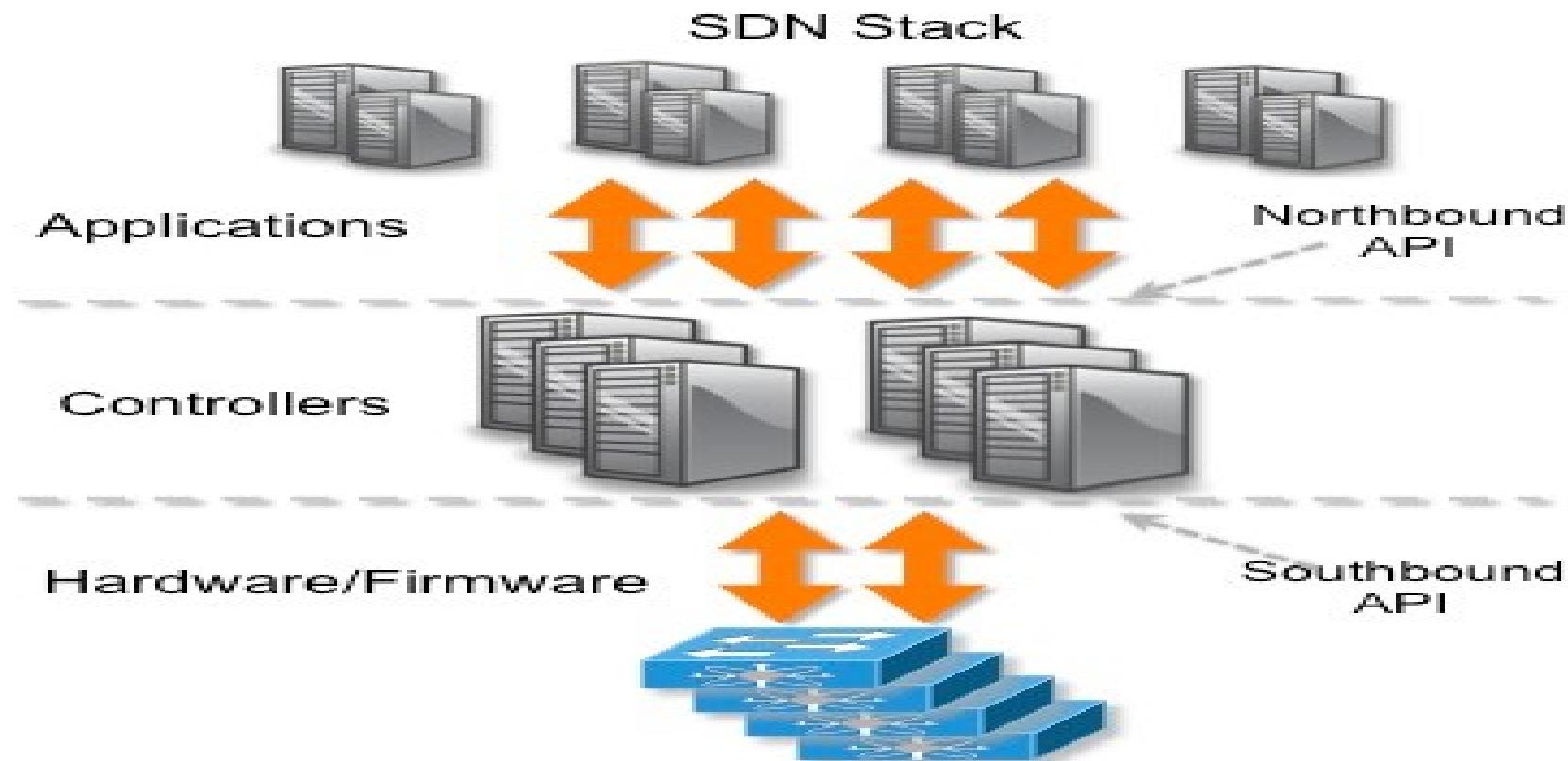
Separation of control plane and data plane

Today's Network vs. SDN



Northbound and southbound APIs

- Enterprise [data center](#)
 - Northbound APIs include management solutions for automation and orchestration, and the sharing of actionable data between systems.
 - Southbound APIs include communication with the switch fabric, [network virtualization](#) protocols, or the integration of a [distributed computing](#) network.



CCNA R&S: Exam code: 200-125

Exam Sample Questions

Lesson 42



Exam Practice Websites

- www.cisco.com
- www.9tut.com
- Books – Review questions
- Lots of lab practice....
& Best of effort

CCNA R&S: Exam code: 200-125

Mock Interview (KC)

Lesson 43



Mock Interview

- Personality Development i.e. Sharpen the SAW
 - Gestures & Posters
 - Grooming i.e. dress, hair dress, first impression – eye contact
- Professional Development
 - Technical Knowledge
 - Close probes, Open Probes i.e. Packet flow
 - Problem-Solving i.e. TSHOOT skills
 - Approach(2), Method(6), clarity
 - Pressure Handling i.e. 90/110
 - I don't know, Calm & Compose & Saying "NO" to yourself
 - Customer's Focus i.e. WIN-WIN
 - Listening Skills – Seek to be understand, then to be understood
 - Types
 - Passive (Store & Think)
 - Active (Intelligence – Being in Present moment no cloud computing)



Grading index

- Tell me, about – Your self
 - Professional Development
 - Technical Knowledge (10)
 - Problem-Solving (10)
 - Pressure Handling (5)
 - Customer's Focus (5)
- Total Marks = 30 points

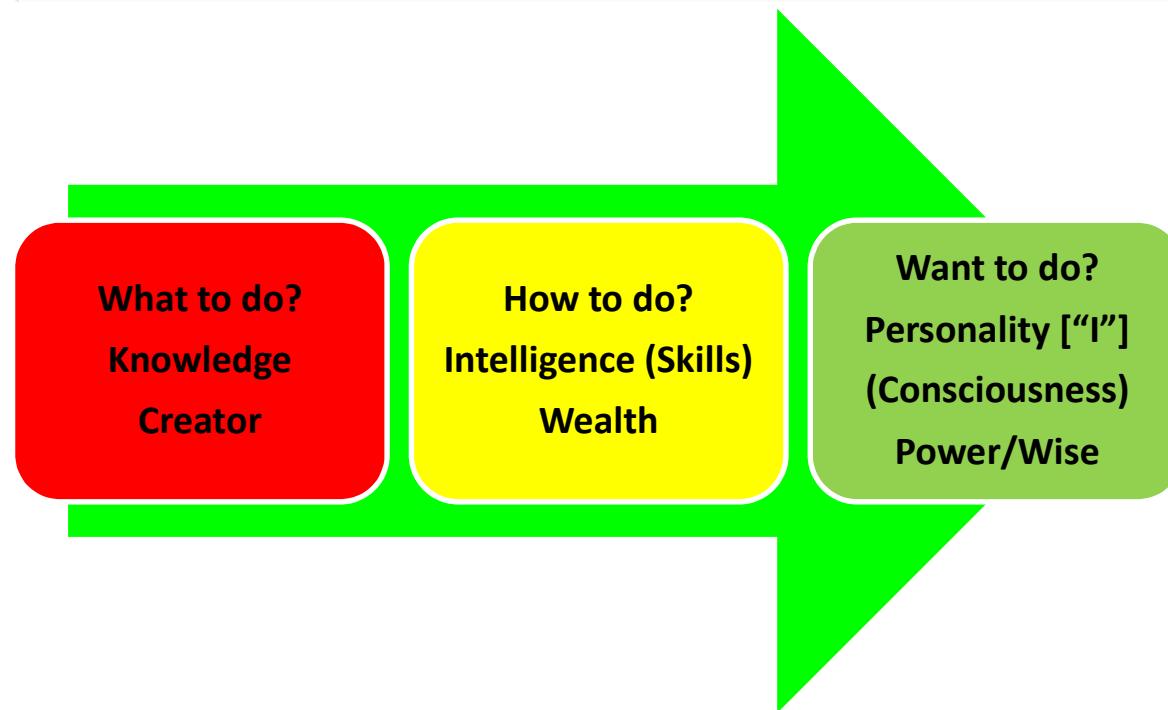
Strength Areas (Skills)	Areas to be Improved



Questions & Answers (Max-15 Mins)



Length of flower is based on water level;
Height of human beings are based on their
own Thoughts i.e. OPM >>> Thiruvallur



= HABIT

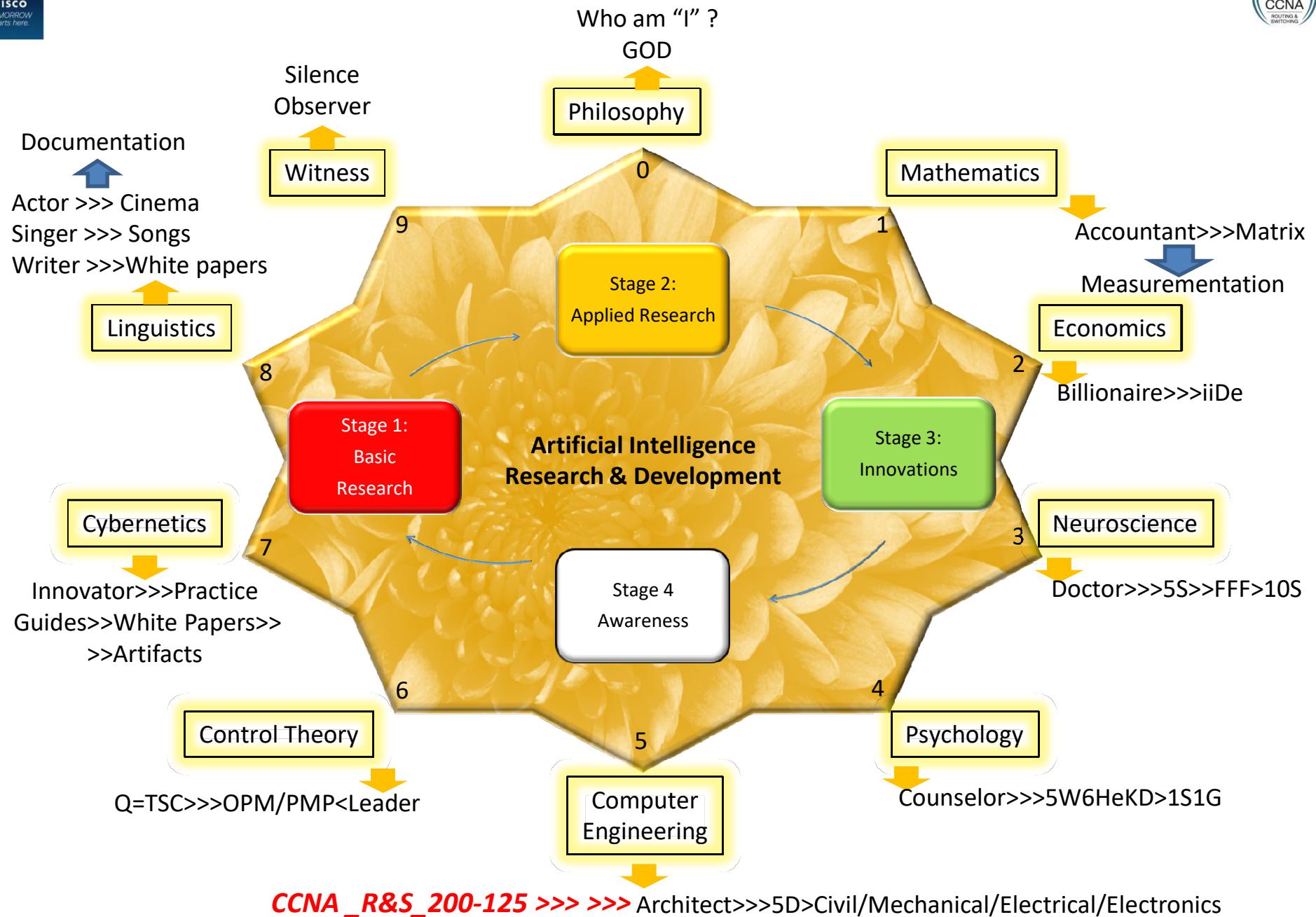
Measurement & Documentation are the
two eyes of Living People >>> Thiruvallur



Kumar's Ai Domain Practices

0. PHI	- Vision: The GOD - Answer for Who am "I"? Mission: Karma Yoga, Bhagavath Gita, Thiruvatasam, Thirumandiram
1. MAT	- Vision: The Accountant – Daily Accounts Mission: Matrix > Q=TSC
2. ECO	- Vision: The Billionaire i.e. b2B Mission: iiDe – Micro vs. Macro – ai_S2_G_V_4.5L_M_1LS
3. NEU	- Vision: The Doctor Mission: Ayurveda, FFF-5S, Gym, Ayurveda, Sattvic Cooking
4. PSY	- Vision: The Counselor [PC – 5W6HeKD Model] Mission: Thirukural
5. COM	- Vision: The Architect {CCAr} Mission: A+, N+, SEC+, S+, MCSE, RHCE, VCP, Python, CCIE[R&S, SEC, SP, DC, COL]
6. CON	- Vision: The Associate Partner Mission: Premium Sales & International Digital Marketing
7. CYB	- Vision: The Innovator Mission: Practice Guides & ai Agents {apps}
8. LIN	- Vision: The Artist Mission:
9. WIT	- Role: The Observer – Responsibility : Awareness





Commonly used TCP and UDP default ports

• TCP ports

- FTP – 20, 21
- SSH – 22
- TELNET – 23
- SMTP – 25
- DNS – 53
- HTTP – 80
- POP3 – 110
- IMAP4 – 143 {Internet Mail Access Protocol}
- HTTPS – 443

What is a port number?

Logical Interface for Applications [L7 Protocols]

IANA {Internet Assigned Numbers Authority}

- Range 0 – 65,535
- Three Blocks
 - Well known ports 0 - 1023
 - Registered ports: 1025 – 49,151
 - Dynamic or Private ports: 49,152 – 65,535

• UDP ports

- TFTP – 69 (IOS Image & Device Configuration Backup(storage))
- NTP – 123 (Time Sync of devices)
- DNS – 53
- BOOTPS/DHCP – 67 (Automatic configure IP, SM, DG, Domain Name & Leased Period)
- SNMP – 161 (Grabs Statistics{i.e. CPU & RAM %} from Devices)

• To verify:

- PC - CMD> netstat

<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>



kumar6009@gmail.com



@air.ds2

Confidential and Need base circulation only

www.kumar6009.wixsite.com/ais3 466