CCNA په پښتو ژبه

CCNA (Cisco Certified Network Associate) in Pashto

ترتيب كوونكي: انجينر عبدالرحيم وِقّاد

فهرست

CCNA د **Cisco Certified Network Associate** لنډیز دی CCNA .د Cisco د مسلکي تصدیقونو په لړۍ کې د پیل او بنسټیزې کچې تصدیق دی. که څوک غواړي د شبکې په برخه کې مسلکي پرمختګ وکړي، CCNAد دې مسلکي مسیر د پیل لپاره مهم بنسټ ګڼل کېږي .

CCNAد Cisco شبکو او د شبکې اړوند بنسټیزو مفاهیمو د زده‌کړې لپاره جوړ شوی، او د دې تصدیق له لارې زده‌کوونکی د شبکې د ټکنالوژیو، Cisco وسایلو او د شبکې د کار کولو له بنسټیزو اصولو سره بلدتیا پیدا کوي.

Network Devicesد شبکې وسایل

د شبکې وسایل هغه تجهیزات دي چې د شبکې د جوړولو، د وسایلو د نښلولو، د معلوماتو د لېږد، د شبکې د مدیریت او د امنیت د تأمین لپاره کارول کېږي. د **CCNA 200-301** د موضوعاتو له مخې، د Network Components په برخه کې روټرونه، Layer 2اوLayer 3 Switches ، Next-Generation Firewallsاو IPS ، Access Points، Controllers، Endpointsاو Servers شامل دي.

1 Router روټر

Routerهغه شبکه‌ییز وسیله ده چې د بېلابېلو شبکو ترمنځ د معلوماتو د لېږد لپاره کارول کېږي.

روټر د شبکې په جوړښت کې د مختلفو شبکو ترمنځ د ارتباط لپاره مهم رول لري. د بېلګې په توګه، یو روټر کولای شي د یوې داخلي شبکې ترافیک د بلې شبکې یا انټرنېټ پر لوري ولېږي.

روټر د **Layer 3**په کچه کار کوي او د IP معلوماتو پر بنسټ د Packet د لېږد لپاره پرېکړه کوي.

په شبکو کې روټرونه د **Default Router/Gateway**په توګه هم کارول کېدای شي. که په یوه Subnet کې څو روټرونه موجود وي، د شبکې د Availabilityد لوړولو لپاره د **First Hop Redundancy Protocol (FHRP)**څخه هم استفاده کېدای شي.

2 Layer 2 Switch — Layer 2

Layer 2 Switchد LAN دننه د Endpoints د نښلولو لپاره کارول کېږي.

د Campus LAN په جوړښت کې **Access Layer Switches**مستقیماً لهEndpoints ، لکه User Devices اوServers ، سره نښلول کېږي.

Layer 2 Switchد Ethernet Frame د لېږد لپاره د **MAC Address**معلومات کاروي.

په ساده ډول:

Endpoint ⟶ Layer 2 Switch ⟶ Network

3 Layer 3 Switch سویچ

Layer 3 Switchد Switching ترڅنګ د Layer 3 Routing وړتیا هم لري.

د شبکې د ډیزاین له مخې، ځینې Switches یوازې د Layer 2 Switching لپاره کارول کېږي، خو Layer 3 Switch کولای شي د IP پر بنسټ د Packet د Routingدندې هم ترسره کړي.

په ځینو شبکو کې حتی Access Layer هم د Layer 3 Switching پر بنسټ جوړېدای شي، چې دې ته **Routed Access Layer**ویل کېږي.

---

4 Access Point (AP) د بېسیم شبکې وسیله

Access Point (AP)د Wireless Network لپاره کارول کېږي.

APد Wireless Endpoints لپاره د شبکې د لاسرسي زمینه برابروي. د مثال په توګه، Laptop، Smartphoneیا بل Wireless Device کولای شي د Access Pointله لارې LAN ته وصل شي.

په **SOHO**شبکو کې ممکن یوه واحده وسیله څو دندې په ګډه ترسره کړي؛ لکه:

- Router
- Switch
- Wireless Access Point
- Firewall

5 Firewall فایروال

Firewallد شبکې د امنیت لپاره کارول کېږي.

Firewallد Network Traffic په مسیر کې قرار نیسي او پرېکړه کوي چې کوم Traffic باید **Allow**او کوم باید **Discard**شي.

Firewallکولای شي د لاندې معلوماتو پر اساس Traffic وڅېړي:

- Source IP Address
- Destination IP Address
- TCP/UDP Port Numbers
- Application-levelمعلومات
- د اړیکې مخکینی حالت(**Stateful Inspection**)

د Router د ACL په پرتله Firewall د Packet Filtering لپاره پراخ امنیتي امکانات لري.

6 IPS Intrusion Prevention System

IPSد شبکې د امنیت یوه وسیله ده چې د شبکې په تېرېدونکي Traffic کې د احتمالي بریدونو د پېژندلو او مخنیوي لپاره کارول کېږي.
Traditional IPS د **Exploit Signatures**له Database څخه استفاده کوي IPS .د Packet معلومات د موجودو Signatures سره پرتله کوي او که معلومه کړي چې Traffic د یوه برید برخه ده، کولای شي:

- Eventثبت کړي؛
- Packetرد کړي؛
- یا Traffic د نورو امنیتي تحلیلونو لپاره Redirect کړي.

IPSد بېلګې په توګه د **DoS**، **DDoS**، **Worms**او **Viruses** په څېر ګواښونو د پېژندلو لپاره کارول کېدای شي.

7 Controller کنټرولر

په Controller-Based Networking کې **Controller**د شبکې د وسایلو د ځینو کنټرولي دندو مرکزي مدیریت ترسره کوي.
د کتاب له مخې، Controllerکولای شي د Network Devices د Control Plane ځینې یا ټولې دندې مرکزي کړي Network Devices .بیا د Controller سره د ارتباط لپاره Interface کاروي چې **Southbound Interface (SBI)**بلل کېږي.
په CCNA کې د Controller مهم مثالونه:

- **Cisco DNA Center**
- **Wireless LAN Controller (WLC)**

8 Endpoint پای‌وسایل

Endpointهغه وسایل دي چې د شبکې د خدماتو د کارولو لپاره له شبکې سره نښلول کېږي.
د مثال په توګه:

- User Devices
- PCs
- Laptops
- نورClient Devices

په Campus LAN کې Access Layer Switches د Endpoints سره مستقیمه اړیکه جوړوي.

9 Serverسرور

Serverد شبکې پر نورو وسایلو او کارووونکو باندې Services او Resources وړاندې کوي.
د Campus LAN په جوړښت کې Servers هم د هغو **Endpoint Devices**له ډلې څخه دي چې Access Layer Switches ورسره مستقیم اتصال جوړوي.

د Network Devices لنډه کتنه

اصلي دنده	وسیله
د بېلابېلو شبکو ترمنځRouting	**Router**
د LAN دننه د Ethernet Frames لېږد او د Endpoints نښلول	**Layer 2 Switch**
Layer 3 RoutingاوSwitching	**Layer 3 Switch**
Wireless Devicesله شبکې سره نښلول	**Access Point**

اصلي دنده	وسيله
د Network Traffic امنيتيFiltering	**Firewall**
د شبکې د بريدونو پېژندل او مخنيوی	**IPS**
د شبکې د وسايلو مرکزي کنټرول او مديريت	**Controller**
د شبکې د خدماتو کارووڼکي وسايل	**Endpoint**
د شبکې Services او Resources وړاندې کول	**Server**

Introduction to Network Topologies د شبکې د توپولوژۍ پېژندنه

Network Topology هغه اصطلاح ده چې د شبکې د وسايلو او د هغوی ترمنځ د ارتباطاتو د جوړښت او ترتيب لپاره کارېږي. د شبکې د ډيزاين پر مهال وسايل په تصادفي ډول له يو بل سره نه نښلول کېږي؛ بلکې د اړتيا، د شبکې د اندازې او د ارتباطاتو د اړتياوو له مخې مناسب Topology انتخابېږي.

په **CCNA 200-301** کې د Network Topology Architecture موضوع د Network Fundamentals برخه ده او د شبکې د Topology د ګانګړتياوو پېژندنه پکې شامله ده.

د Network Topology مهم ډولونه

په کتاب کې د LAN Design لپاره لاندې عمومي Topology اصطلاحات بيان شوي دي:

۱. Star Topology — ستوري توپولوژي

په **Star Topology** کې يو مرکزي Network Device له ځو نورو وسايلو سره مستقيمې اړيکې لري.

که د مرکزي وسيلې ځخه د نورو وسايلو پر لوري د ارتباطاتو کرښې رسمې شي، جوړښت د ستوري په ځېر ښکاري؛ له همدې امله ورته **Star Topology** ويل کېږي.

د Campus LAN په Access Layer کې Access Switch او له هغه سره نښلول شوي Endpoints د Star Topology يوه بېلګه جوړوي.

---

۲. Full Mesh Topology — بشپړه Mesh توپولوژي

په **Full Mesh** کې د شبکې د هرې جوړې Nodes ترمنځ مستقيم Link موجود وي.

يعنې که ځو Network Nodes موجود وي، هر Node له نورو ټولو Nodes سره مستقيمه اړيکه لري.

د دې جوړښت مهمه ګانګړتيا دا ده چې د Nodes ترمنځ د ارتباطاتو شمېر ډېرېږي. د مثال په توګه، د ۴۲ Nodes لپاره Full Mesh د **861 Links** اړتيا لري، چې د Switch Ports مصرف هم ډېر زياتوي.

---

۳. Partial Mesh Topology — نيمګړې Mesh توپولوژي

په **Partial Mesh** کې د شبکې د ټولو Nodes ترمنځ مستقيم Link نه وي؛ بلکې يوازې د ځينو Nodes ترمنځ مستقيمې اړيکې موجودې وي.

په بل عبارت:

Partial Mesh = Mesh، خو Full Mesh نه وي.

په دوه‌پوړيز Campus LAN کې د Access او Distribution Switches ترمنځ معمولاً **Partial Mesh** کارول کېږي.

د بېلګې په توګه، که هر Access Switch له دوو Distribution Switches سره وصل وي، خو ټول Access Switches له يو بل سره مستقيم وصل نه وي، نو دا Partial Mesh ده.

---

۴. Hybrid Topology — ګډه توپولوژي

Hybrid Topology هغه ډيزاين دی چې د ځو مختلفو Topology مفاهيم په يوه لوی او عموماً پېچلي Network Design کې سره يوځای کړي.

دوه‌پوړيز Campus LAN د Hybrid Topology يوه بېلګه ده، ځکه:

- **Access Layer** ⟶ Star Topology
- **Distribution Layer** ⟶ Partial Mesh

نو دواړه سره يوځای د **Hybrid Design** جوړښت رامنځته کوي.

د Campus LAN او Topology اړيکه

د Campus LAN په ډيزاين کې Cisco د Switches لپاره درې مهمې طبقې يا Layers کاروي:

Access ⟶ Distribution ⟶ Core

د دوی دندې له یو بل سره توپیر لري Access Switches .له End Users سره مستقیمه اړیکه لري، Distribution Switchesد Access Switches لپاره د ترافیک د ټېرېدو مسیر برابروي، او Core Switches په لویو Campus LANs کې Distribution Switches سره نښلوي.

دوه‌پوړیزه‌Topology

Two-Tier Designدوه Layers لري:

Access Layer + Distribution Layer

په دې ډیزاین کې End Devices د Access Switches سره نښلول کېږي، او Access Switches له Distribution Switches سره ارتباط لري. د Access او Distributionترمنځ عموماً Partial Mesh کارول کېږي.

دا ډیزاین د **Collapsed Core**په نوم هم یادېږي، ځکه چې Core Layer نه لري او Core وظیفه د Distribution Layer سره یوځای شوې وي.

درې‌پوړیزه‌Topology

Three-Tier Designدرې Layers لري:

Access ⟶ Distribution ⟶ Core

په دې ډیزاین کې Core Switches د Distribution Switches ترمنځ د ارتباط لپاره کارول کېږي. دا جوړښت په لویو Campus LANs کې د شبکې د پراختیا او د Switch Ports او Cables د اغېزمن استعمال لپاره ګټور دی.

لنډه پایله

د Network Topology هدف دا دی چې وښیي **Network Devices څنګه له یو بل سره نښلول شوي او Network Design څنګه جوړ شوی دی.**

په دې برخه کې مهم Topology ډولونه دا دي:

اساسي مفهوم	Topology
یو مرکزي Device له ځو نورو Devices سره نښلول کېږي	**Star**
هر Node له هر بل Node سره مستقیم Link لري	**Full Mesh**
یوازې ځینې Nodes له یو بل سره مستقیم Links لري	**Partial Mesh**
د ځو Topology ډولونو ګډDesign	**Hybrid**

په Campus LAN کې **Two-Tier Design**عموماً د **Star + Partial Mesh**ګډ جوړښت لري، نو د **Hybrid Topology**مثال ګڼل کېږي.

د Network Protocols پېژندنه

Network Protocolsیا **د شبکې پروتوکولونه** هغه ټاکل شوي اصول او میتودونه دي چې د شبکې وسایل او کمپیوټرونه یې د معلوماتو د تبادلې لپاره کاروي. د CCNA کتاب په **TCP/IP**چاپېریال کې ښلاښل پروتوکولونه تشریح کوي چې هر یو یې د شبکې د اړیکو ځانګړې دنده ترسره کوي.

TCP/IP Protocol Suite

TCP/IPد پروتوکولونو یوه مجموعه ده چې د IP شبکو د جوړولو او د مختلفو Hosts ترمنځ د معلوماتو د لېږد لپاره کارول کېږي. د TCP/IP په دې مجموعه کې **TCP**او **IP**تر ټولو مشهور پروتوکولونه دي.

د Network Protocols د پوهېدو لپاره مهمه خبره دا ده چې هر Protocol ځانګړې دنده لري؛ ځینې د معلوماتو د اعتبار وړ انتقال لپاره، ځینې د نومونو د IP Addressسره د تړلو لپاره، او ځینې دWeb ، File Transferاو Network Management لپاره کارول کېږي.

مهم TCP/IP پروتوکولونه

1. TCP ـــ Transmission Control Protocol

TCPیو **Connection-Oriented Transport Layer Protocol**دی چې د معلوماتو د باوري انتقال لپاره کارول کېږي.

TCPد معلوماتو د انتقال پر مهال د لاندې کارونو ملاتړ کوي:

- Connection Establishment
- Ordered Data Transfer
- Error Recovery
- Reliability
- Flow Control

TCPد Sequence او Acknowledgment معلومات کاروي ترڅو د معلوماتو د انتقال حالت معلوم او د اړتیا په صورت کې د معلوماتو د بیا لېږلو امکان برابر کړي.

2. UDP — User Datagram Protocol

UDPهم د TCP/IP د Transport Layer پروتوکول دی، خو د TCP په څېر Connection-Oriented نه دی.

ITCPاو UDP د Application Data د انتقال لپاره کارول کېږي، او د **Port Numbers**له لارې مشخصوي چې ترلاسه شوي معلومات باید د کوم Applicationته وسپارل شي.

3. IP — Internet Protocol

IPد شبکې په جوړښت کې د Hosts ترمنځ د Packet د انتقال لپاره کارول کېږي.

د IPv4 په Packet کې د **Protocol Field**موجود دی چې مشخصوي د IPv4 Header وروسته کوم Transport Protocol راځي. د مثال په توګه:

- **6 = TCP**
- **17 = UDP**

نو Receiving Host د IP Header له دې معلوماتو څخه استفاده کوي ترڅو پوه شي چې د IP Packet دننه TCP دی که.UDP

4. DNS — Domain Name System

DNSیو **Application Layer Protocol**دی چې Hostname د هغه اړوند IP Address سره ترجمه کوي.

د مثال په توګه، Clientکولای شي د یوه Web Server نوم وغواړي او DNS Server یې اړوند IP Address پیدا کړي.

5. HTTP — Hypertext Transfer Protocol

HTTPد Web Client او Web Server ترمنځ د Web Files د انتقال لپاره کارول کېږي.

کله چې Browser د Web Server سره TCP Connection جوړ کړي، بیا د Web Page د ترلاسه کولو لپاره HTTP کاروي. د HTTP مشهور Request د **GET** Requestدی.

6. DHCP — Dynamic Host Configuration Protocol

DHCPد Client وسایلو لپاره د IP Address او نورو مهمو IP Settings د ترلاسه کولو لپاره کارول کېږي.

DHCP Serverد Client لپاره د IP Address Lease برابروي او نور اړین Network Settings هم ورکولی شي.

7. FTP — File Transfer Protocol

FTPد Network له لارې د Files د انتقال لپاره کارول کېږي.

FTPد TFTP په پرتله ډېر امکانات لري او د File Transfer لپاره د Client او Server ترمنځ ارتباط برابروي.

8. TFTP — Trivial File Transfer Protocol

TFTPد Files د انتقال لپاره یو ساده Application Protocol دی.

Ciscoوسایل کولای شي له TFTP څخه د Files د انتقال لپاره استفاده وکړي. د TFTP Server لپاره **UDP Port 69**کارول کېږي.

9. SSH — Secure Shell

SSHد Remote Access لپاره کارېدونکی Protocol دی او په CCNA کې د TCP/IP Application Protocols له ډلې څخه دی.

SSHد **TCP Port 22**کاروي.

10. Telnet

Telnetهم د Remote Access لپاره کارول کېږي او د **TCP Port 23**څخه استفاده کوي.

11. SNMP — Simple Network Management Protocol

SNMPد Network Devices د Management او Monitoring لپاره یو **Application Layer Protocol**دی.

Network Management Softwareکولای شي د SNMP له لارې د Network Devices معلومات ترلاسه او د شبکې د فعالیت وضعیت وڅاري.

12. SMTPاوPOP3

SMTPاو **POP3**د Email اړوند پروتوکولونه دي. د کتاب له مخې، دواړه د معلوماتو د باوري انتقال اړتیا لري، نو **TCP**کاروي.

مهم Protocolsاو Port Numbers

Protocol	دنده	Port	Transport
FTP	File Transfer	20/21	TCP
SSH	Remote Access	22	TCP
Telnet	Remote Access	23	TCP

Transport	Port	دنده	Protocol
TCP	25	Email Transfer	**SMTP**
TCP/UDP	53	Name Resolution	**DNS**
UDP	67	IP Configuration	**DHCP Server**
UDP	68	IP Configuration	**DHCP Client**
UDP	69	File Transferساده	**TFTP**
TCP	80	Web	**HTTP**
TCP	110	Email	**POP3**
UDP	161	Network Management	**SNMP**
UDP	514	Network Logging	**Syslog**

IP Address

IP Address (Internet Protocol Address)هغه منطقي يا Logical Address دی چې په Network کې د يوه Device د پېژندلو او له نورو Devices سره د Communicationلپاره کارېږي.

هر هغه Device چې په IP Network کې Communication کوي، لکه:

- Computer
- Laptop
- Server
- Router
- Printer
- IP Camera
- Smartphone

کولی شي IP Address ولري.

د IP Address اصلي دنده دا ده چې Network ته وښيي:

کوم Device بايد د معلوماتو ترلاسه کوونکی وي او معلومات بايد کومې Network برخې ته ولېږل شي.

د IP Address اهميت

فرض کړئ په يوه Network کې درې Computers موجود دي:

PC1 ⟶ 192.168.1.10

PC2 ⟶ 192.168.1.20

PC3 ⟶ 192.168.1.30

که PC1 غواړي PC2 ته معلومات ولېږي، Networkبايد پوه شي چې د معلوماتو مقصد: 192.168.1.20

دی.

نو IP Address د Network Communication لپاره د Device د منطقي پېژندنې په توګه کار کوي.

IPv4 Address

IPv4 (Internet Protocol Version 4)د IP Address يوه ډېره کارېدونکې نسخه ده.

IPv4 Addressاد **32 bits**څخه جوړ شوی وي.

دا 32 bits په څلورو برخو وېشل کېږي چې هره برخه يې **Octet**بلل کېږي.

IPv4 Address څنګه جوړ شوی؟

IPv4د **32 bits**څخه جوړ دی:

192.168.1.10

هره برخه 8 bits لري.

په مجموع کې 32 bits = 8 + 8 + 8 + 8 :

Network Portion اوHost Portion

په IPv4 Address کې دوه مهمې برخې شته:

Network Portion

دا ښيي چې Device د کوم Network برخه ده.

Host Portion

دا په هماغه Network کې ځانګړی Device پېژني.

مثلاً:

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

دلته:

Network = 192.168.1.0

Host = 10

نو 192.168.1.10په Network 192.168.1.0کې يو Host دی.

Subnet Mask

Subnet Mask موږ ته ښيي چې د IP Address کومه برخه **Network**ده او کومه برخه **Host**ده.

مثال:

IP Address: 192.168.1.10 Subnet Mask: 255.255.255.0 د /24په شکل هم ليکل کېږي

دلته /24معنا لري چې د IP Address لومړني **24 bits**د Network لپاره دي.

Network Address

Network Addressد يوه Network د پېژندلو لپاره کارېږي.

مثلاً:

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Network Address:

192.168.1.0

دا Address عموماً يوه ځانګړې Host ته نه ورکول کېږي.

Broadcast Address

Broadcast Addressد يوه Network ټولو Hosts ته د معلوماتو د لېږلو لپاره کارېږي.

د:

192.168.1.0/24

Network Broadcast Address:

192.168.1.255

مثلاً که يو Device Broadcast واستوي، د همدې Network ټول مناسب Hosts يې ترلاسه کولی شي.

Usable Host Addresses

په Network 192.168.1.0/24کې:

Network Address = 192.168.1.0

Broadcast = 192.168.1.255

نو د Hosts لپاره:Usable Addresses

192.168.1.1

تر 192.168.1.254 يعني ټول: 254 Usable Hosts

Public او Private IP Address

IPv4 Addressesد استعمال له مخې په مختلفو ډولونو وېشل کېږي.

Private IP Address

Private IP Address'sپه داخلي يا Local Networks کې کارېږي.

مهم:Private IPv4 Ranges

Range	Private Network
10.0.0.0 – 10.255.255.255	10.0.0.0/8
172.16.0.0 – 172.31.255.255	172.16.0.0/12
192.168.0.0 – 192.168.255.255	192.168.0.0/16

مثال 192.168.1.10 :دا Private IP دی.

Public IP Address

Public IP Addressهغه IP Address دی چې په Public Internet کې د Internet-routable Communication لپاره کارېږي.

مثلاً يو Router کولی شي له ISP څخه Public IP ترلاسه کړي او د هغې لاړې Internet ته وصل شي.

Static او Dynamic IP Address

Static IP

Static IPهغه IP دی چې په ثابت ډول Device ته Configuration کېږي.

مثلاً192.168.1.10: Server :

که Administrator هغه واتي، IPيې نه بدلېږي.

Static IPعموماً په لاندې Devices کې ډېر کارېږي:

- Servers
- Routers
- Network Printers
- IP Cameras
- Network Infrastructure Devices

Dynamic IP

Dynamic IPد **DHCP (Dynamic Host Configuration Protocol)**له لارې په اتومات ډول Device ته ورکول کېږي.

مثال :کله چې PC Network ته وصل شي، DHCP Serverورته IP Address او نور Network Parameters ورکوي.

12. Default Gateway

Default GatewayهغهDeviceعموماًRouter ، دی چې Host يې د خپل Local Network څخه بهر د Traffic لېږلو لپاره کاروي.

که PC غواړي د خپل Network څخه بهر کوم Address ته معلومات ولېږي، Trafficد Default Gateway له لارې استوي.

د IP Address يو بشپړ عملي مثال

فرض کړئ يو PC داسې Configuration لري:

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 8.8.8.8

په Cisco Router کې د IP Address Configuration

فرض کړئ:Router Interface GigabitEthernet0/0 ته دا IP Address ورکوو:

192.168.1.1/24

Configuration:

```
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
```

د Interface حالت معلومولو لپاره:

```
Router# show ip interface brief
```

مثلاً نتیجه:

```
Interface IP-Address Status
GigabitEthernet0/0 192.168.1.1 up
```

MAC Address

MAC Address (Media Access Control Address)د شبکې د یوه Device د **Network Interface**لپاره یو ځانګړی Address دی. دا Address په **Data** **Link Layer (Layer 2)**کې کارول کېږي.

MAC Addressد Ethernet شبکو په switching کې ډېر مهم دی، ځکه چې **Switch**د **MAC Address پر بنسټ Frames** له یوه Port څخه بل Port ته لېږي. د Cisco کتاب په Port Security کې هم MAC Address د Switch Port سره د Device د پېژندلو او امنیت لپاره کاروي.

د MAC Address بڼه

MAC Address عموماً **48-bit**وي، یعنې **6 Bytes**لري.

مثال 00:11:22:33:44:55

MAC Address په Switch کې

کله چې یو Device د Switch له Port سره وصل شي، Switchکولی شي د هغه **Source MAC Address** Device زده کړي او په **MAC Address Table**کې یې ثبت کړي.

مثلاً:

MAC Address	Port
0011.2233.4455	Fa0/1
0022.3344.5566	Fa0/2

بیا Switch د همدې جدول پر بنسټ پوهېږي چې کوم MAC Address په کوم Port کې دی.

MAC Addressاو IP Address

IP Address	MAC Address
Layer 3کې کارېږي	Layer 2کې کارېږي
د Network/Host منطقي پېژندنه	د Network Interface پېژندنه
Routerيې د Routing لپاره کاروي	Switchيې د Switching لپاره کاروي
مثال192.168.1.10 :	مثال0011.2233.4455 :

MAC Addressپه Port Security کې

Cisco Switchکولی شي مشخص MAC Address د یوه Port لپاره **Secure MAC Address**وټاکي.

مثلا Switch(config-if)# switchport port-security mac-address 0011.2233.4455:

په دې حالت کې Switch ټاکل شوی MAC Address د هغه Port لپاره مجاز ګڼي. که بل MAC Address د Port له لارې راشي، **Port Security Violation** رامنځته کېدای شي.

Sticky MAC Address

Switchکولی شي MAC Address په اتومات ډول زده او په Running Configuration کې يې ثبت کړي:

```
Switch(config-if)# switchport port-security mac-address sticky
```

د کتاب له مخې، Sticky Learningد Device Source MAC Address زده کوي او د Port Security په Configuration کې يې اضافه کوي.

Port Address

Port Addressپه Networking کې هغه **Port Number**ته ويل کېږي چې د **TCPيا UDP** په وسيله د يوه Device دننه د ځانګړي Application يا Network Serviceد پېژندلو لپاره کارېږي.

د CCNA کتاب له مخې، Applicationsد **Well-Known Port Number**څخه استفاده کوي، ترڅو Client پوه شي چې کوم Port ته بايد Connection جوړ کړي.

Port Number

Port Numberد **16-bit**ارزښت دی او له **0څخه تر 65,535** پورې شمېرې لري.

مثال: Protocol: TCP Port Number: 80 IP Address: 192.168.1.10

دلته Deviceد IP Address 192.168.1.10لري او د HTTP Service لپاره د **Port 80**کاروي.

مشهورPort Numbers

Application	Protocol	Port Number
FTP Data	TCP	20
FTP Control	TCP	21
SSH	TCP	22
Telnet	TCP	23
SMTP	TCP	25
DNS	TCP/UDP	53
DHCP Server	UDP	67
DHCP Client	UDP	68
TFTP	UDP	69
HTTP	TCP	80
POP3	TCP	110
SNMP	UDP	161
SSL/HTTPS	TCP	443
Syslog	UDP	514

دا Well-Known Port Numbers د CCNA کتاب په جدول کې هم ذکر شوي دي.

Destination PortاوSource Port

کله چې Client له Server سره ارتباط جوړوي، Packet/Segmentکې **Source Port**او **Destination Port**دواړه موجود وي.

مثال:

Client Web Server

192.168.1.10 192.168.1.20

Source Port: 49172 Destination Port: 80

دلته: **Source Port = 49172** ⟶ Client موقتي Port

Destination Port = 80 ⟶ Web Server HTTP Serviceد

Protocol = TCP

Port Addressولې مهم دی؟

یوازې **IP Address**نه شي ویلای چې په Device کې کوم Application ته معلومات ورسېږي.

مثلاً:

192.168.1.10:80

192.168.1.10:22

192.168.1.10:53

IP Addressیو شان دی، خو Port Number مختلف دی؛ نو هر Port کولی شي د مختلف Service/Connection استازیتوب وکړي.

Introduction to OSI, TCP/IP, and Cisco Three-Layer Hierarchical Model

1. OSI Model

Model **OSI (Open Systems Interconnection)**یو **Reference Model**دی چې د Network Communication د کارونو د تشریح او تنظیم لپاره کارېږي.

OSI Modelشبکه په **7 Layers**وېشي. هر Layer ځانګړی وظیفه لري او د Network Communication په بهیر کې له نورو Layers سره تعامل کوي.

د OSI Model اووهLayers

Layer	نوم	اساسي دنده
7	Application	Network Servicesاو Applications ته خدمتونه
6	Presentation	Data Format، Translationاو Encryption
5	Session	Sessionجوړول، ساتل او ختمول
4	Transport	End-to-End Delivery، Reliabilityاو Flow Control
3	Network	Logical Addressingاو Routing
2	Data Link	Framesاو MAC Addressing
1	Physical	Bits، Cablesاو Physical Signals

په CCNA کې د Layer Number کارول ډېر مهم دي. د مثال په توګه، **Transport Layer = Layer 4**دی، او TCP او UDP د TCP/IP Stack په Transport Layerکې کار کوي.

2. TCP/IP Model

Model **TCP/IP (Transmission Control Protocol/Internet Protocol)**هغه Networking Model دی چې د TCP/IP Protocol Suite د کار کولو طریقه تشریح کوي.

TCP/IP Modelد OSI Model په پرتله لږ Layers لري او د Internet او Modern Networks په عملي کار کې ډېر مهم دی.

TCP/IP Model Layers

د OSI سره نږدې ارتباط	TCP/IP Layer
OSI Layers 5, 6, 7	Application
OSI Layer 4	Transport
OSI Layer 3	Internet
OSI Layers 1, 2	Network Access

Transport Layer

TCP/IP Modelکې **Transport Layer**د End-to-End Communication لپاره مهمې دندې ترسره کوي.

د دې Layer مشهورProtocols:

- **TCP**
- **UDP**

TCPد **Error Recovery**، **Reliability**، **Flow Control**او **Ordered Data Transfer**په څېر خدمات وړاندې کوي، په داسې حال کې چې UDP نسبتاً ساده دی او دا ټول خدمات نه وړاندې کوي.

د OSI او TCP/IP دواړو Models کې Transport Layer د **Layer 4**په توګه پېژندل کېږي.

Cisco Three-Layer Hierarchical Model .3

Cisco Three-Layer Hierarchical Modelد Enterprise/Campus Network د ډیزاین لپاره یو Hierarchical Design دی.

دا Network په درې اصلي Layers وېشي:

1. **Access Layer**
2. **Distribution Layer**
3. **Core Layer**

Access Layer 3.1

Access Layerهغه Layer دی چې **End Devices**ورسره مستقیم نښلي.

لکه:

- PC
- Laptop
- IP Phone
- Server

Access Switchesد End-User Devices لپاره د Network Connection Point برابروي او Distribution Layer ته هم متصل کېږي.

Distribution Layer 3.2

Distribution Layerد Access Switches لپاره **Aggregation Point**دی.

د دې Layer مهم کارونه:

- Access Switchesسره نښلول
- Traffic Aggregation
- د Network مختلفو برخو ترمنځ Connectivity برابرول
- Framesد Switches ترمنځ Forward کول

Distribution Layerعموماً په مستقیم ډول End-User Devices نه نښلوي.

Core Layer 3.3

Core Layerد لوی Campus Network مرکزي Layer دی.

د Core Layer اصلي دنده دا ده چې **Distribution Switches**له یو بل سره وصل کړي او د لوی مقدار Network Traffic لپاره لوړ سرعت Connectivity برابر کړي.

د درې واړو Layers مهم توپیر

اصلي دنده	Layer
End Devicesنښلوي	**Access**
Access Layersسره نښلوي او Aggregation برابروي	**Distribution**
Distribution Layersسره نښلوي او لوړ سرعت Connectivity برابروي	**Core**

Router and Switch Hardware, Ports, and Boot-Up Process

Router Hardware .1

Routerیو Network Device دی چې د **Layer 3**په کچه کار کوي او د IP Address پر بنسټ د مختلفو Networks ترمنځ Packets Forward کوي.

د Router مهم Hardware Components عبارت دي له:

- **CPU (Central Processing Unit)**
- **RAM**
- **ROM**

- **NVRAM**
- **Flash Memory**
- **Network Interfaces/Ports**
- **Console Port**
- **USB Ports**په ځينو Models کې

2. Switch Hardwar

Switchعموماً د **Layer 2**په کچه کار کوي او د MAC Address پر بنسټ Ethernet Frames Forward کوي.

د Switch مهم Hardware Components عبارت دي له:

- **CPU**
- **RAM**
- **Flash Memory**
- **Interfaces/Ports**
- **ASIC**
- **TCAM**

په Cisco Switch کې د Data Plane د Frame Forwarding لپاره **ASIC**کارول کېږي. ASIC د MAC Address Table د چټک Lookup لپاره له **TCAM**سره کار کوي. Switch بيا CPU او RAM هم لري چې IOS او د Control/Management Plane اړوند کارونه ترسره کوي.

3. Router and Switch Ports

Port/Interfaceهغه فزيکي يا منطقي Connection Point دی چې Network Device پرې له بل Device سره ارتباط جوړوي.

مهم Ports اوInterfaces

استعمال	Port / Interface
د Ethernet Network اتصال	Ethernet
د لوړ سرعت Ethernet اتصال	Gigabit Ethernet
په ځينوRouterونو کې WAN Connection	Serial
د Device د CLI Management لپاره	Console
د USB Flash او ځينو Management/Storage کارونو لپاره	USB

Console Port

Console Portد Router يا Switch د مستقيم Management لپاره کارېږي، په ځانګړي ډول کله چې Network Connection لا نه وي تنظيم شوی.

د Cisco CLI له لارې Administrator Commands داخلوي او Device د هغو Commands په ځواب کې Output ورکوي.

4. Router Boot-Up Process

کله چې **Power On** Cisco Router يا **Reload**شي، د Boot-Up Process په عمومي ډول په څلورو مرحلو ترسره کېږي.

Step 1: POST

POST (Power-On Self-Test)د Router Hardware معاينه کوي.

Routerګوري چې Hardware Components په سمه توګه کار کوي که نه.

Step 2: Bootstrap

Routerله **ROM**څخه Bootstrap Program ته Copy کوي او هغه اجرا کوي.

Step 3: IOS Loading

Bootstrap Programتاکي چې کوم **IOS Image**بايد Load شي.

IOSعموماً له **Flash Memory**څخه RAM ته Load کېږي.

که مناسب IOS ونه موندل شي، Routerکولای شي **ROMMON**ته لاړ شي.

Step 4: Startup Configuration

کله چې IOS Running شي، Routerد **startup-config**فايل پيدا کوي او هغه **RAM**ته د **running-config**په توګه Load کوي.

NVRAM

د حافظو مهم توپير

مهم استعمال	Memory
POSTاوBootstrap	ROM
IOS، Running Configurationاو فعال معلومات	RAM
IOS Imageذخیره کول	Flash
Startup Configurationذخیره کول	NVRAM

Cisco Routerکې startup-configپه NVRAMکې ساتل کېږي، په داسې حال کې چې running-configپه RAMکې وي.

Boot-Up مهم ترتیب:

POST ⟶ Bootstrap ⟶ IOS ⟶ Startup-config ⟶ Running-config

Switch Modes – Basic Configuration

Cisco IOSکې د Switch Configuration لپاره بېلابېل **Modes**کارول کېږي. هر Mode خپل ځانګړی Prompt او Commands لري.

1. User EXEC Mode

Prompt:

```
Switch>
```

په دې Mode کې د Switch لومړني Commands کارول کېږي.

له User EXEC Mode څخه Privileged EXEC Mode ته:

```
Switch> enable
```

2. Privileged EXEC Mode

Prompt:

```
Switch#
```

په دې Mode کې د Switch د کتنې او Management لپاره Commands کارول کېږي.

مهمCommands

```
Switch# show running-config
Switch# show startup-config
Switch# show version
Switch# show ip interface brief
Switch# show vlan brief
Switch# show mac address-table
Switch# show cdp neighbors
Switch# copy running-config startup-config
Switch# write memory
Switch# show clock
```

له Privileged EXEC Mode څخه **Global Configuration Mode**ته د تګ لپاره:

```
Switch# configure terminal
```

3. Global Configuration Mode

Prompt:

```
Switch(config)#
```

په دې Mode کې د Switch عمومي Configuration ترسره کېږي.

مثالونه

```
Switch(config)# hostname SW1
Switch(config)# enable secret Cisco123
Switch(config)# banner motd #
Switch(config)# ip default-gateway 192.168.1.1
Switch(config)# clock timezone AFT 4 30
```

4. Console Configuration Mode

Prompt:

```
Switch(config-line)#
```

د Console Line د Configuration لپاره کارېږي.

مثال

```
Switch(config)# line console 0
Switch(config-line)# password Cisco123
Switch(config-line)# login
Switch(config-line)# exit
```

5. Interface Configuration Mode

Prompt:

```
Switch(config-if)#
```

د Switch د يوه ځانګړي Interface يا Port د Configuration لپاره کارېږي.

مثال

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
```

مهمه يادونه: د Cisco IOS په Configuration کې Prompt ته پام کول ډېر مهم دي، ځکه هر Command يوازې په ځانګړي Mode کې اجرا کېدای شي. د ورکړل شوي CCNA موادو له مخې، د Configuration او Verification لپاره د CLI عملي مهارتونه هم مهم دي.

Network Troubleshooting Commands

Network Troubleshooting Commands هغه Commands دي چې د Network د ستونزو د معلومولو، د IP Configuration د کتلو، د Connectivity د ازمېښت، د DNS د بررسی او د Routing معلوماتو د کتلو لپاره کارېږي.

د ورکړل شوي CCNA کتاب له مخې، د Network Troubleshooting لپاره لاندې Commands مهم دي.

1. Ipconfig

Mode: Windows CMD

```
C:\> ipconfig
```

تشریح:

د کمپیوټر مهم IPv4 معلومات ښکاره کوي، لکه:

- IP Address
- Subnet Mask
- Default Gateway

مثال:

```
Ethernet adapter:

   IPv4 Address . . . . . : 192.168.1.10
   Subnet Mask  . . . . . : 255.255.255.0
   Default Gateway . . . : 192.168.1.1
```

د دې Command له لارې معلومولای شو چې Computer صحیح IP Configuration لري که نه.

2. ipconfig /all

```
C:\> ipconfig /all
```

تشریح:

د ipconfigپه پرتله ډېر تفصیلي Network معلومات ښکاره کوي.

پکې معمولاً دا معلومات لیدل کېږي:

- IP Address
- Subnet Mask
- Default Gateway
- DNS Server
- DHCPمعلومات
- MAC Address

دا Command د Host د بشپړ IPv4 Configuration د بررسی لپاره ګټور دی.

3. ping

Mode: Windows CMD / Cisco IOS

```
C:\> ping 192.168.1.1
```

په Cisco Device کې:

```
Switch# ping 192.168.1.1
```

تشریح:

pingد دوو Network Devices ترمنځ **Connectivity**ازمویي.

که مقصد Device ځواب ورکړي، معمولاً داسې نتیجه وینو:

```
Reply from 192.168.1.1:
bytes=32 time<1ms TTL=64
```

pingد Network Troubleshooting له مهمو لومړنیو Commands څخه دی. د کتاب له مخې، pingاو tracerouteد ACLs او Network Connectivity په Troubleshootingکې هم کارول کېږي.

4. tracert

Mode: Windows CMD

```
C:\> tracert 8.8.8.8
```

تشریح:

tracertښیي چې Packet د خپل مقصد تر رسېدو پورې له کومو **Routers/Hops**څخه تېرېږي.

دا Command هغه وخت ګټور دی چې pingناکام شي او غواړو معلومه کړو چې ستونزه د Network په کومه برخه کې ده.

5. traceroute

Mode: Cisco IOS

```
Switch# traceroute 8.8.8.8
```

په Router کې هم:

```
Router# traceroute 8.8.8.8
```

تشریح:

په Cisco Devices کې tracerouteد Windows د tracertپه څېر د Packet مسیر معلوموي.

د کتاب په موادو کې pingاو tracerouteد Network Troubleshooting لپاره د عملي Testing وسیلو په توګه یاد شوي دي.

6. nslookup

Mode: Windows CMD

```
C:\> nslookup google.com
```

تشریح:

nslookupد **DNS**د بررسی لپاره کارېږي.

دا معلوموي چې Domain Name کوم IP Address ته Resolve کېږي.

مثال:

Name: google.com

Address: 142.250.190.14

کله چې Website د Domain Name له لارې نه خلاصيږي، nslookupمرسته کوي چې د DNS Resolution ستونزه معلومه کړو.

7. arp -a

Mode: Windows CMD

C:\> arp -a

تشریح:

دا Command د **ARP Table** ښکاره کوي.

په ARP Table کې د IP Address او اړوند MAC Address اړیکه لیدل کیږي.

مثال:

Internet Address Physical Address

192.168.1.1 00-11-22-33-44-55

د دې Command له لارې معلومولای شو چې Host د Local Network د Devices لپاره کوم MAC Address زده کړی دی. د کتاب په Command Referenceکې هم arp -a شامل دی.

8. netstat

Mode: Windows CMD

C:\> netstat

تشریح:

netstatد Computer فعالې Network Connections او Listening Ports د کتلو لپاره کاربړي.

netstat -a

C:\> netstat -a

تشریح:

Active Connectionsاو Listening Ports ښکاره کوي.

netstat -r

C:\> netstat -r

تشریح:

د **Routing Table** Computer ښکاره کوي.

netstat -n

C:\> netstat -n

تشریح:

Network Connectionsد IP Address او Port Number په عددي بڼه ښکاره کوي، پرته له دې چې Domain Names ته يې Resolve کړي.

د کتاب په موادو کې netstat -rnهم د Host د IPv4 Routing Table د کتلو لپاره ښودل شوی.

د Network Troubleshooting Commands لنډ جدول

اصلي استعمال	Platform	Command
IP، Maskاو Gateway کتل	Windows	ipconfig
بشپړNetwork Configuration	Windows	ipconfig /all
Connectivityازمويل	Windows / Cisco	ping
د Packet مسير معلومول	Windows	tracert
د Packet مسير معلومول	Cisco	traceroute
DNS Resolutionازمويل	Windows	nslookup
ARP Tableکتل	Windows	arp -a
Network Connectionsکتل	Windows	netstat

اصلي استعمال	Platform	Command
Active اوListening Ports	Windows	netstat -a
Routing Table	Windows	netstat -r
Numeric Network Connections	Windows	netstat -n

دا Commands د Network ستونزې په مرحلەوار ډول د معلومولو لپاره کارول کېږي.

Switch Telnet and SSH Configuration

په Cisco Switch کې **Telnet**او **SSH**د **Remote Management**لپاره کارېږي. د کتاب له مخې، دواړه د **Management Plane**پروتوکولونه دي **Telnet** . معلومات او Password په غیررمز شوې بڼه لېږي، خو **SSH**د خوندي Remote Management لپاره کارول کېږي.

1. Telnet Configuration

د Telnet لپاره Switch باید Management IP ولري او VTY Lines ته د Telnet اجازه ورکړل شي.

د Telnet بشپړConfiguration

```
Switch> enable
Switch# configure terminal

Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.2 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# ip default-gateway 192.168.1.1

Switch(config)# line vty 0 4
Switch(config-line)# password Cisco123
Switch(config-line)# login
Switch(config-line)# transport input telnet
Switch(config-line)# exit

Switch(config)# end

Switch# copy running-config startup-config
```

د مهمو Commands تشریح

Management IP:

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.2 255.255.255.0
Switch(config-if)# no shutdown
```

Switchته Management IP ورکوي.

Default Gateway:

```
Switch(config)# ip default-gateway 192.168.1.1
```

کله چې Remote Management له بلې شبکې څخه ترسره کېږي، Default Gatewayکارول کېږي.

VTY Lines:

```
Switch(config)# line vty 0 4
```

د Remote Login لپاره VTY Lines ټاکي.

Password:

```
Switch(config-line)# password Cisco123
```

د Telnet Login Password ټاکي.

Login:

```
Switch(config-line)# login
```

د VTY Password د Login لپاره فعالوي.

Transport Input:

```
Switch(config-line)# transport input telnet
```

يوازې **Telnet** Remote Connectionته اجازه ورکوي.

له PC څخه Telnet Connection

که د Switch IP Address 192.168.1.2 وي:

```
C:\> telnet 192.168.1.2
```

بيا:

```
Password: Cisco123
Switch>
```

---

2. SSH Configuration

SSH (Secure Shell) د Switch لپاره خوندي Remote Management برابروي. د کتاب له مخې، SSH د Telnet په پرتله غوره انتخاب دی، ځکه Telnet ټول معلومات په غيررمز شوې بڼه لېږي.

د SSH Configuration

1. Enable Secret

```
Switch> enable
Switch# configure terminal
Switch(config)# enable secret Cisco123
```

د Privileged EXEC Mode لپاره Password ټاکي.

2. Hostname

```
Switch(config)# hostname SW1
```

د Switch نوم SW1 ټاکي.

3. Domain Name

```
SW1(config)# ip domain-name company.local
```

د SSH د RSA Encryption Key جوړولو لپاره Domain Name تنظيموي.

4. Management IP Address

```
SW1(config)# interface vlan 1
SW1(config-if)# ip address 192.168.1.2 255.255.255.0
SW1(config-if)# no shutdown
SW1(config-if)# exit
```

Switchته Management IP Address ورکوي.

5. Default Gateway

```
SW1(config)# ip default-gateway 192.168.1.1
```

له بلې شبکې څخه د SSH Management لپاره Default Gateway تنظيموي.

6. Generate RSA Key

```
SW1(config)# crypto key generate rsa
```

کله چې پوښتنه وکړي:

```
How many bits in the modulus [512]:
```

وليکئ:

```
2048
```

دا د SSH لپاره RSA Key جوړوي.

7. SSH Version 2

```
SW1(config)# ip ssh version 2
```

SSH Version 2فعالوي.

8. Local User Account

```
SW1(config)# username admin secret Cisco123
```

د SSH Login لپاره Local Username او Password جوړوي.

9. Allow SSH on VTY Lines

```
SW1(config)# line vty 0 4
SW1(config-line)# transport input ssh
```

یوازې SSH Connection ته اجازه ورکوي.

که دواړه **SSHاو Telnet** فعالول غواړئ:

```
SW1(config-line)# transport input ssh telnet
```

10. Local Login

```
SW1(config-line)# login local
```

Switchته وایي چې د Login لپاره Local Username او Password وکاروي.

11. Save Configuration

```
SW1(config-line)# exit
SW1(config)# end
SW1# copy running-config startup-config
```

یا:

```
SW1# write memory
```

د SSH بشپړConfiguration

```
Switch> enable
Switch# configure terminal

Switch(config)# hostname SW1
SW1(config)# enable secret Cisco123
SW1(config)# ip domain-name company.local

SW1(config)# interface vlan 1
SW1(config-if)# ip address 192.168.1.2 255.255.255.0
SW1(config-if)# no shutdown
SW1(config-if)# exit

SW1(config)# ip default-gateway 192.168.1.1

SW1(config)# crypto key generate rsa
How many bits in the modulus [512]: 2048

SW1(config)# ip ssh version 2
SW1(config)# username admin secret Cisco123

SW1(config)# line vty 0 4
SW1(config-line)# transport input ssh
SW1(config-line)# login local
SW1(config-line)# exit

SW1(config)# end
SW1# copy running-config startup-config
```

Telnetاو SSH مهم توپیر

SSH	Telnet	ځانګړنه
22	23	TCP Port
هو	هو	Remote Management
هو	نه	معلومات رمز کوي؟
هو	نه	Passwordخوندي لېږدوي؟

غوره انتخاب کمزوری انتخاب د Production Network لپاره

Telnetټول معلومات unencrypted لېږي؛ له همدې امله د عملي شبکو لپاره **SSH**غوره دی.

Switch Port Security

Port Security د Cisco Switch یو **Layer 2 Security Feature**دی چې د Switch په Access Port کې د **MAC Address**پر بنسټ کنټرول کوي چې کومه وسیله له Port څخه Network ته لاسرسی ولري. که یوه نااشنا MAC Address د ټاکل شوې پالیسۍ خلاف Port ته راشي، Switchد ټاکل شوي **Violation Mode**مطابق عمل کوي.

د Port Security ګټې

Port Securityد لاندې موخو لپاره کارېږي:

- د غیرمجاز کمپیوټرونو مخنیوی
- د MAC Address Flooding په څېر بریدونو پر وړاندې د Port ساتنه
- د Network Security زیاتول
- په Access Port کې د مجازوMAC Address ونو کنټرول

د Port Security فعالولو شرط

Port Securityپه **Access Port**کې تنظیمېږي؛ نو لومړی باید Port د Access Mode په توګه تنظیم شي.

دPort Security Configuration

فرض کړئ:

- Port: FastEthernet0/1
- یوازې یوComputer
- Sticky MAC
- Violation Mode: Shutdown

1. Interface .ته داخلېدل

```
Switch> enable
Switch# configure terminal
Switch(config)# interface fastethernet0/1
```

2. Port Access Mode .ته اړول

```
Switch(config-if)# switchport mode access
```

3. Port Security .فعالول

```
Switch(config-if)# switchport port-security
```

4. MAC Addressونو Maximum شمېر ټاکل

```
Switch(config-if)# switchport port-security maximum 1
```

دا Port ته یوازې **یوه MAC Address** اجازه ورکوي.

5. Sticky MAC .فعالول

```
Switch(config-if)# switchport port-security mac-address sticky
```

Switchد Port څخه د وسیلې MAC Address زده کوي او د Port Security د Secure MAC Address په توګه یې په **running-config**کې ثبتوي. د Configurationد خوندي کولو لپاره باید copy running-config startup-configوکارول شي.

6. Violation Mode تاکل.

```
Switch(config-if)# switchport port-security violation shutdown
```

7. Configuration خوندي کول.

```
Switch(config-if)# end
Switch# copy running-config startup-config
```

د Port Security بشپړ Configuration

```
Switch> enable
Switch# configure terminal

Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security violation shutdown

Switch(config-if)# end
Switch# copy running-config startup-config
```

Port Security Violation Modes

کله چې نااشنا MAC Address د Port Security له پالیسۍ سره مخالفت وکړي، درې مهم Violation Modes شته:

1. Protect

```
Switch(config-if)# switchport port-security violation protect
```

- نااشنا MAC Address ردوي.
- Portفعال پاتې کېږي.
- Logنه جوړوي.

2. Restrict

```
Switch(config-if)# switchport port-security violation restrict
```

- نااشنا MAC Address ردوي.
- Portفعال پاتې کېږي.
- **Counter**زياتوي.
- **Log**جوړوي.

3. Shutdown

```
Switch(config-if)# switchport port-security violation shutdown
```

دا د **Default Violation Mode** د Port Security دی.

کله Violation رامنځته شي:

- Portد **err-disabled**حالت ته ځي.
- Trafficپه Port کې بندېږي.
- Portتر بیا فعالولو پورې کار نه کوي.

د Violation Modes لنډه پرتله

Log / Counter	Port	د نااشنا MAC سره چلند Mode
نه	فعال پاتې کېږي	MACردوي Protect
هو	فعال پاتې کېږي	MACردوي Restrict

Log / Counter	Port	د نااشنا MAC سره چلند Mode
Violationثبتوي err-disabled	Portبندوي	Shutdown

Port Security Verification Commandsد

1.د ټولو Port Security معلومات

```
Switch# show port-security
```

د Switch د Port Security عمومي وضعيت ښيي.

2.د يوه مشخص Port معلومات

```
Switch# show port-security interface fastethernet0/1
```

د مشخص Port د Port Security Configuration او اوسني Status تفصيلي معلومات ښيي.

3. Secure MAC Addresses

```
Switch# show port-security address
```

ټول Secure MAC Addresses ښکاره کوي.

4. Running Configuration

```
Switch# show running-config
```

د Port Security تنظيمات په Running Configuration کې ښيي.

5.دPort Status

```
Switch# show interfaces status
```

که Port د Port Security Violation له امله بند شوی وي، د err-disabledحالت ليدل کېدای شي.

د Shutdown Port بيا فعالول

که Port د Port Security Violation له امله err-disabledشوی وي:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
```

Shutdown او بيا no shutdownد Interface د بيا فعالولو لپاره کارول کېږي.

Sticky MACپاکول

```
Switch(config-if)# no switchport port-security mac-address sticky
```

يا د Interface Secure Sticky MAC پاکولو لپاره:

```
Switch# clear port-security sticky interface fastethernet0/1
```

DHCP, DHCP Snooping and DHCP Relay Agent

1. DHCP

DHCP (Dynamic Host Configuration Protocol)د دې لپاره کارېږي چې Network Devices ته په اتومات ډول د Network اړين معلومات ورکړي، لکه **IP Address**او نور اړوند معلومات.

کله چې Client د DHCP له لارې Address اخلي، Switchد DHCP پيغامونو معلومات تحليلولای شي او د Client اړوند معلومات په **DHCP Snooping Binding Table**کې ثبتوي.

2. DHCP Snooping

DHCP Snoopingد Cisco Switch يو **Security Feature**دی چې د DHCP پيغامونه ځاري او د DHCP د غيرمجاز استعمال پر وړاندې Network ساتي.

د DHCP Snooping يو مهم هدف دا دی چې د **Fake DHCP Server**له لارې د Client لپاره ناسم IP Address يا Gateway ورکولو مخه ونيسي.

Untrusted PortsاوTrusted

DHCP Snooping Portsپه دوو برخو وېشي:

Trusted Port

هغه Port چې د اصلي DHCP Server يا DHCP Relay Agent پر لوري وي.

```
Switch(config)# interface fa0/1
Switch(config-if)# ip dhcp snooping trust
```

Untrusted Port

نور Ports په Default ډول **Untrusted**وي؛ نو د Untrusted لپاره ځانګړی Command ته اړتیا نشته.

د کتاب په مثال کې د DHCP Relay Agent سره وصل Port Trusted دی، او د PC Ports د Default Untrusted حالت کې پاتې کېږي.

3. DHCP Snooping Configuration

Step 1 : DHCP Snoopingفعالول

```
Switch> enable
Switch# configure terminal
Switch(config)# ip dhcp snooping
```

دا په Switch کې DHCP Snooping فعالوي.

Step 2: په VLAN کې DHCP Snooping فعالول

```
Switch(config)# ip dhcp snooping vlan 10
```

دا DHCP Snooping په VLAN 10 کې فعالوي.

د کتاب له مخې، دا دواړه Global Commands د DHCP Snooping د فعالېدو لپاره اړین دي.

Step 3: Trusted Portټاکل

```
Switch(config)# interface fa0/1
Switch(config-if)# ip dhcp snooping trust
```

دا **Trusted** Port کوي.

Step 4: Rate Limit

```
Switch(config)# interface fa0/2
Switch(config-if)# ip dhcp snooping limit rate 10
```

دا په یوه ثانیه کې د DHCP پیغامونو شمېر محدودوي. د DHCP Snooping Rate Limiting د DHCP Message Flooding پر وړاندې د ساتنې لپاره کارول کېږي.

Step 5: Configurationخوندي کول

```
Switch(config-if)# end
Switch# copy running-config startup-config
```

د DHCP Snooping بشپړ مثال

```
Switch> enable
Switch# configure terminal

Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10

Switch(config)# interface fa0/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# exit

Switch(config)# interface range fa0/2-24
Switch(config-if-range)# ip dhcp snooping limit rate 10

Switch(config-if-range)# end
Switch# copy running-config startup-config
```

4. DHCP Snooping Binding Table

DHCP Snooping د DHCP پیغامونو څخه د Client معلومات اخلي او په **DHCP Snooping Binding Table** کې یې ثبتوي.

په دې Table کې د Client لپاره د **MAC Address**، **IP Address**، **Lease**، **VLAN**او **Interface** په څېر معلومات ليدل کېږي.

د Binding Table د کتلو:Command

```
Switch# show ip dhcp snooping binding
```

مثال:

```
MacAddress IpAddress VLAN Interface
02:00:11:11:11:11 172.16.2.101 11 Gi1/0/3
02:00:22:22:22:22 172.16.2.102 11 Gi1/0/4
```

5. DHCP Snooping Verification Commands

DHCP Snooping Statusد

```
Switch# show ip dhcp snooping
```

د Trusted Ports معلومات

```
Switch# show ip dhcp snooping interface
```

Binding Tableد

```
Switch# show ip dhcp snooping binding
```

---

6. DHCP Relay Agent

کله چې **DHCP Server**په بل **Subnet/Network کې وي**، DHCP Clientنشي کولی خپل DHCP Broadcast په مستقیم ډول Router ته واړوي، ځکه Routerعموماً Broadcast بلې شبکې ته نه Forward کوي.

د دې ستونزې د حل لپاره **DHCP Relay Agent**کارول کېږي.

Routerد DHCP Client غوښتنه DHCP Server ته Forward کوي.

7. DHCP Relay Configuration

Interfaceته داخلېدل

```
Router> enable
Router# configure terminal

Router(config)# interface g0/0
```

DHCP Relayفعالول

```
Router(config-if)# ip helper-address 10.10.10.2
```

ip helper-address د DHCP Client غوښتنې د DHCP Server پر لوري Forward کوي.

Interfaceفعالول

```
Router(config-if)# no shutdown
```

Configurationخوندي کول

```
Router(config-if)# exit
Router(config)# end
Router# copy running-config startup-config
```

د DHCP Relay بشپړ مثال

```
Router> enable
Router# configure terminal
Router(config)# interface g0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# ip helper-address 10.10.10.2
Router(config-if)# no shutdown
Router(config-if)# exit
```

```
Router(config)# end
Router# copy running-config startup-config
```

DHCP Relay Verification

```
Router# show running-config
```

يا:

```
Router# show ip interface g0/0
```

DHCP Snooping او DHCP Relay Agent توپير

DHCP Relay Agent	DHCP Snooping
DHCPغوښتنې بلې شبکې ته Forward کوي	د DHCP امنیت زیاتوي
د مختلفوSubnet ونو ترمنځ DHCP ممکن کوي	د Fake DHCP Server پر وړاندې مرسته کوي
په Router یا Layer 3 Switch کې Configuration کېږي	په Switch کې Configuration کېږي
ip helper-addressکاروي	Trusted/Untrusted Portsکاروي
DHCP Serverته Client غوښتنه Forward کوي	Binding Tableجوړوي

VLANs

VLAN (Virtual Local Area Network) د Switch په دننه کې د شبکې د منطقي وېش لپاره کارېږيVLAN. ونه مرسته کوي چې په یوه فزیکي Switch کې وسایل په جلا منطقي شبکو ووېشل شي.

د بېلګې په توګه، یو Switch کولای شو داسې تنظیم کړو:

VLAN 10 ⟶ IT

VLAN 20 ⟶ HR

VLAN 30 ⟶ Finance

په دې ډول دIT ، HRاو Finance وسایل په جلاVLAN ونو کې تنظیمېږي.

1. د VLAN جوړول

د VLAN جوړولو لپاره Global Configuration Mode ته داخلېږو:

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name IT
```

د بل VLAN لپاره:

```
Switch(config)# vlan 20
Switch(config-vlan)# name HR
```

2. Access Port ورکول VLANته

کله چې VLAN جوړ شي، باید Port مشخص VLAN ته Assign شي.

مثلاً FastEthernet0/1د VLAN 10 برخه کول:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
```

دلته:

```
switchport mode access
```

Portد Access Mode ته اړوي.

```
switchport access vlan 10
```

Portد VLAN 10 سره نښلوي.

3.څو Ports یو VLAN ته Assign کول

که غواړو څو Ports په یو ځل VLAN 10 ته Assign کړو:

```
Switch(config)# interface range fastethernet0/1-10
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
```

په دې توګه Fa0/1تر Fa0/10پورې ټول Ports د VLAN 10 برخه کېږي.

4. Trunk Port

کله چې د دووSwitch ونو ترمنځ د څوVLAN ونو Traffic انتقالول غواړو، **Trunk Port**کارول کېږي.
مثلاً:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode trunk
```

SwitchدTrunk Link ونو ترمنځ د VLAN Traffic انتقال لپاره کارول کېږي.

5. VLAN Verification

دVLAN ونو د کتلو لپاره:

```
Switch# show vlan brief
```

دا Command د Switch موجودVLAN ونه او د هغوی اړوند Ports ښيي.

د Trunk د کتلو لپاره:

```
Switch# show interfaces trunk
```

د Interface د Switching معلوماتو لپاره:

```
Switch# show interfaces switchport
```

7.د VLAN بشپړ عملي مثال

فرض کړئ غواړو:

- VLAN 10 = IT
- VLAN 20 = HR
- Fa0/1–10 = IT
- Fa0/11–20 = HR
- G0/1 = Trunk

Configuration:

```
Switch> enable
Switch# configure terminal

Switch(config)# vlan 10
Switch(config-vlan)# name IT
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# name HR
Switch(config-vlan)# exit

Switch(config)# interface range fastethernet0/1-10
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit

Switch(config)# interface range fastethernet0/11-20
Switch(config-if-range)# switchport mode access
```

```
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# exit

Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit

Switch(config)# end
Switch# copy running-config startup-config
```

VTP & LLDP

۱. VTP ـــ VLAN Trunking Protocol

VTP (VLAN Trunking Protocol)د Cisco Layer 2 پروتوکول دی چې د VLAN معلومات دSwitch ونو ترمنځ د **Trunk Link**له لارې انتقالوي، ځو د VLAN Configurationمدیریت اسانه شي.

د VTP ګټې

- پهSwitch ونو کې د VLAN مدیریت اسانه کوي.
- د VLAN Configuration وخت کموي.
- د VLAN معلومات دSwitch ونو ترمنځ انتقالوي.
- د Configuration د انساني تېروتنو احتمال کموي.

د VTP لپاره مهم شرطونه

- Switchونه باید د VTP لپاره مناسب Cisco Switches وي.
- دSwitch ونو ترمنځ **Trunk Link**باید فعال وي.
- Switchونه باید یو شان **VTP Domain Name**ولري.
- VTP Versionباید مناسب/یو شان وي.
- که Password کارول کېږي، باید پهSwitch ونو کې یو شان وي.

VTP Modesد

Server Mode.۱

په **Server Mode**کې VLAN جوړول او بدلول کېږي او VLAN معلومات نوروSwitch ونو ته استول کېږي.

```
Switch(config)# vtp mode server
```

Client Mode.2

په **Client Mode**کې Switch د VLAN معلومات له Server څخه ترلاسه کوي.

```
Switch(config)# vtp mode client
```

Transparent Mode.3

په **Transparent Mode**کې Switch خپلVLANونه په خپله اداره کوي او د VTP پیغامونه Forward کوي.

```
Switch(config)# vtp mode transparent
```

VTP Domain

د VTP Domain د ټاکلو لپاره:

```
Switch(config)# vtp domain CCNA
```

VTP Password

```
Switch(config)# vtp password Cisco123
```

VTP Version

```
Switch(config)# vtp version 2
```

VTP Server Configuration

```
Switch> enable
Switch# configure terminal

Switch(config)# hostname SW1
Switch(config)# vtp mode server
Switch(config)# vtp domain CCNA
Switch(config)# vtp password Cisco123
Switch(config)# vtp version 2

Switch(config)# vlan 10
Switch(config-vlan)# name IT
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# name HR
Switch(config-vlan)# exit

Switch(config)# end
Switch# copy running-config startup-config
```

VTP Client Configuration

```
Switch> enable
Switch# configure terminal

Switch(config)# hostname SW2
Switch(config)# vtp mode client
Switch(config)# vtp domain CCNA
Switch(config)# vtp password Cisco123
Switch(config)# vtp version 2

Switch(config)# end
Switch# copy running-config startup-config
Switch# show vtp status
Switch# show vlan brief
Switch# show interfaces trunk
```

LLDP ـــ Link Layer Discovery Protocol.2

LLDP (Link Layer Discovery Protocol)د Layer 2 Discovery Protocol دی چې Network Device ته اجازه ورکوي د خپل **مستقیم Neighbor Device** په اړه معلومات ترلاسه کړي LLDP .پیغامونه Router یا Switch نه Forward کوي؛ نو یوازې مستقیم Connected Neighbor معلوموي.

LLDPکولی شي د Neighbor په اړه داسې معلومات ښکاره کړي:

- Device Name
- Local Interface
- Neighbor Interface
- Device Capabilities
- Management IP Address
- System Description
- د IOS معلومات

LLDPفعالول

Cisco Devicesکې LLDP په Default ډول **Disabled**وي. د ټولو Interfaces لپاره يې د فعالولو:Command

```
Switch(config)# lldp run
```

LLDPپه يوه Interface کې فعالول

```
Switch(config)# interface gigabitethernet1/0/19
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
```

lldp transmitد LLDP پيغامونه استوي.

lldp receiveد Neighbor څخه ترلاسه شوي LLDP پيغامونه Process کوي.

LLDPغير فعالول

د ټولو Switch لپاره:

```
Switch(config)# no lldp run
```

په Interface کې د Transmit بندول:

```
Switch(config-if)# no lldp transmit
```

د Receive بندول:

```
Switch(config-if)# no lldp receive
Switch# show lldp neighbors
```

دا د هر Neighbor لپاره لنډ معلومات ښيي.

```
Switch# show lldp neighbors detail
```

د ټولو Neighbor Devices تفصيلي معلومات ښکاره کوي.

```
Switch# show lldp entry R1
```

يوازې د R1په نوم Neighbor معلومات ښکاره کوي.

LLDP Timer

د کتاب له مخې:Default LLDP

Send Timer = 30 seconds Hold Time = 120 seconds

د Send Timer بدلول Switch(config)# lldp timer 60:

د Hold Time بدلول Switch(config)# lldp holdtime 180:

VTPاو LLDP لنډ توپير

LLDP	VTP
Neighbor Discovery Protocol	VLAN Management Protocol
د مستقيم Neighbor معلومات معلوموي	د VLAN معلوماتو د مديريت لپاره کارېږي
د Layer 2 پيغامونو له لارې Neighbor کشفوي دSwitch ونو ترمنځ د Trunk له لارې کار کوي	
Transmitاو Receive عمليات لري	Server, Client, Transparent Modesلري
show lldp neighbors	show vtp status

DTP and STP

DTP —— Dynamic Trunking Protocol .1

DTP (Dynamic Trunking Protocol)د Cisco پروتوکول دی چې د دووSwitch ونو ترمنځ د Port حالت په اتومات ډول د **Access**يا **Trunk**په توګه ټاکلو کې مرسته کوي DTP .د Trunk جوړولو لپاره کارېږي.

د DTP ګټې

- Trunkپه اتومات ډول جوړوي.
- د Configuration وخت کموي.
- دSwitch ونو ترمنځ د VLAN Traffic انتقال ممکن کوي.

DTP Modes

1. Dynamic Auto

دا Mode د مقابل Switch ځخه د Trunk غوښتنې انتظار کوي.

```
Switch(config-if)# switchport mode dynamic auto
```

2. Dynamic Desirable

دا Mode په فعاله توګه د Trunk جوړولو هڅه کوي.

```
Switch(config-if)# switchport mode dynamic desirable
```

3. Trunk

Portپه ثابت ډول Trunk کېږي.

```
Switch(config-if)# switchport mode trunk
```

4. Access

Portپه ثابت ډول Access کېږي.

```
Switch(config-if)# switchport mode access
```

5. Disable DTP

DTPپیغامونه بندوي:

```
Switch(config-if)# switchport nonegotiate
```

دا عموماً د Manual Trunk Configuration سره کارول کېږي.

د DTP Modes پایله

پایله	Switch B	Switch A
✗ نه جوړېږي Trunk	Dynamic Auto	Dynamic Auto
✓ جوړېږي Trunk	Dynamic Desirable	Dynamic Auto
✓ جوړېږي Trunk	Dynamic Desirable	Dynamic Desirable
✓ جوړېږي Trunk	Dynamic Auto	Trunk
✓ جوړېږي Trunk	Dynamic Desirable	Trunk
✗ پاتې کېږي هرMode		Access

DTP Trunk Configurationد

```
Switch> enable
Switch# configure terminal

Switch(config)# interface g0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport nonegotiate

Switch(config-if)# end
Switch# copy running-config startup-config
```

2. STP — Spanning Tree Protocol

STP (Spanning Tree Protocol)په Layer 2 شبکو کې د اضافي یا Redundant Links له امله د رامنځته کېدونکو **Loops**مخنیوی کوي.

که په Network کې ځوSwitch ونه د Redundant Links له لارې سره وصل وي، د Layer 2 Frames لپاره Loop رامنځته کېدای شي .STP ځینې Interfacesد Forwarding لپاره محدودوي، ځو Network Loop رامنځته نه شي.

دلته دSwitch ونو ترمنځ درې Links شته .STP د اضافي Layer 2 Path له امله د Loop مخنیوي لپاره یو Port Block کوي.

د STP اساسي هدف

STPد Redundancy ګټه ساتي، خو د Layer 2 Loop مخنیوي لپاره د ځینو Paths د Forwarding مخه نیسي.

3. Root Bridge

په STP کې یو Switch د **Root Bridge** په توګه ټاکل کېږي.

د کتاب د CCNA موضوعاتو له مخې، د STP مهم مفاهیم عبارت دي له:

- Root Bridge
- Root Port
- Designated Port
- Forwarding
- Blocking
- PortFast

4. Root Port

Root Port هغه Port دی چې Non-Root Switch له لارې Root Bridge ته تر ټولو غوره مسیر ترلاسه کوي.

5. Designated Port

Designated Port هغه Port دی چې په یوه Network Segment کې د Forwarding لپاره ټاکل کېږي.

STP د Root Bridge، Root Ports او Designated Ports په ټاکلو سره د Network د Layer 2 Paths اداره کوي.

6. STP Port States

د Port د Network Traffic Forward کوي.

Forwarding = Traffic اجازه لري!

Port Traffic Forward نه کوي، ځو Layer 2 Loop رامنځته نه شي.

Blocking = Traffic Forwarding بند

د CCNA Exam Topics کې **Forwarding** او **Blocking** د STP مهم Port States په توګه شامل دي.

7. PortFast

PortFast د Access Port لپاره کارېږي، په ځانګړي ډول هغه Port چې End Device لکه PC ورسره وصل وي.

د PortFast هدف دا دی چې Access Port ژر د Forwarding حالت ته ورسېږي.

د CCNA Exam Topics کې **PortFast benefits** د STP/Rapid PVST+ له مهمو موضوعاتو څخه دی.

8. RSTP — Rapid Spanning Tree Protocol

RSTP (Rapid Spanning Tree Protocol) د STP چټکه بڼه ده.

د کتاب د CCNA Exam Topics له مخې، د **Rapid PVST+ Spanning Tree Protocol** اساسي عملیات باید وپېژندل شي.

په Campus Network کې STP/RSTP د Redundant Layer 2 Links له امله د Loop مخنیوي لپاره کارول کېږي.

DTP او STP توپیر

STP	DTP
Spanning Tree Protocol	Dynamic Trunking Protocol
د Layer 2 Loop مخنیوی کوي	د Trunk جوړولو لپاره کارېږي
د Layer 2 Paths اداره کوي	د Port حالت د Access/Trunk په توګه ټاکي
Root Bridge او Root Port لري	Dynamic Auto او Dynamic Desirable لري
د Loop مخنیوی د STP له لارې	switchport mode trunk
د STP وضعیت د اړوندو Show Commands له لارې کتل کېږي	show interfaces trunk

Command of DTP

switchport mode trunk
switchport mode access
switchport mode dynamic auto
switchport mode dynamic desirable
switchport nonegotiate

show interfaces trunk
show interfaces switchport

1. EtherChannel

EtherChannelد څو فزيکي Ethernet Links د يو منطقي Link په توګه د يوګای کولو تخنيک دی. د دې له لارې دSwitch ونو ترمنځ **Redundancy**او **Load Balancing**ترلاسه کېږي. د CCNA 200-301 د Exam Topics له مخې، د **Layer 2/Layer 3 EtherChannel**او په ګانګړي ډول **LACP**بايد وپېژندل شي او Configure/Verify شي.

وه يا څو فزيکي Links د يوه منطقي **Port-Channel**په توګه کار کوي.

د EtherChannel مهمې ګټې

- **Redundancy:**که يو Link خراب شي، نور Links کار ته دوام ورکوي.
- **Load Balancing:** Trafficد موجودو Links ترمنځ وېشل کېږي.
- **Bandwidth:**څو فزيکي Links يوګای د منطقي Channel برخه جوړوي.
- **STP:** EtherChannelد STP لپاره د يوه Logical Link په توګه ليدل کېږي. د کتاب په Campus LAN مثال کې د Layer 2 EtherChannels د Load Balancingاو Redundancy لپاره کارول شوي دي.

2. LACP

LACP (Link Aggregation Control Protocol)د EtherChannel د جوړولو لپاره کارول کېږي. د CCNA Exam Topics په ګانګړي ډول د **EtherChannel** Configuration **(LACP)**او Verification غوښتنه کوي.

LACP Modes

Active

Switchپه فعاله توګه د LACP EtherChannel د جوړولو هڅه کوي.

channel-group 1 mode active

Passive

Switchد LACP پيغامونو انتظار کوي.

channel-group 1 mode passive

د EtherChannel د جوړولو لپاره **Active + Active**يا **Active + Passive**کارول کېدای شي.

3. EtherChannel Configuration

فرض کړئ د دووSwitch ونو ترمنځ دا Ports کاروو:

Switch> enable
Switch# configure terminal
Switch(config)# interface range fa0/1-3
Switch(config-if-range)# channel-group 1 mode active
Switch(config-if-range)# exit
witch(config)# interface port-channel 1
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
Switch# copy running-config startup-config
Switch2 Configrantion
Switch> enable
Switch# configure terminal
Switch(config)# interface range fa0/1-3

```
Switch(config-if-range)# channel-group 1 mode active
Switch(config-if-range)# exit
Switch(config)# interface port-channel 1
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
Switch# copy running-config startup-config
```

په دې Configuration کې درې فزيکي Ports د **Port-Channel 1** په يوه منطقي EtherChannel کې شاملېږي.

EtherChannel Verification.4

Port-Channelمعلومات

```
Switch# show etherchannel summary
```

د EtherChannel مفصل معلومات

```
Switch# show etherchannel
```

Port-Channel Interface

```
Switch# show interfaces port-channel 1
```

Trunkمعلومات

```
Switch# show interfaces trunk
```

د CCNA لپاره د EtherChannel Configuration تر ځنګ د **Verification**مهارت هم مهم دی.

---

5. Switch Stacking

Switch Stackingهغه طريقه ده چې څو فزيکيSwitch ونه د Stack په توګه سره نښلول کېږي، څو د Network په مديريت کې د يوه منطقي Switch په څېر اداره کېدای شي.

د Stack په جوړښت کې څوSwitch ونه د ځانګړو **Stack Connections/Cables**له لارې سره نښلول کېږي.

په دې ډول څوSwitch ونه د يوه Stack په توګه تنظيمېږي.

د Switch Stacking مهمې ګټې

1. Centralized Management

دStack Switch ونه د يوه منطقي سيسټم په توګه اداره کېدای شي.

2. Scalability

د Network د پراخېدو پر وخت اضافي Switch د Stack برخه کېدای شي.

3. Redundancy

د Stack جوړښت دSwitch ونو ترمنځ د اضافي ارتباطاتو له لارې د Availability په زياتولو کې مرسته کوي.

4.سادهManagement

د څو جلاSwitch ونو پر ځای د Stack د منطقي سيسټم مديريت اسانه کېږي.

SPAN — Switch Port Analyzer

SPAN (Switched Port Analyzer)د Cisco Switch يوه ځانګړنه ده چې د يوه يا څو **Source Ports/VLANs**څخه Network Traffic کاپي کوي او يوه ټاکل شوې **Destination Port**ته يې لېږي. Destination Port عموماً د **Packet Analyzer**وسيله لکه Wireshark يا د Network Monitoring وسيله نښلول کېږي.

يادونه: په ورکړل شوي CCNA 200-301 Official Cert Guide, Volume 2کې د SPAN د Configuration تفصيلي برخه نه ده موندل شوې؛ نو لاندې تشريح د SPANد Cisco IOS عام مفهوم دی، نه د همدې کتاب مستقيم استخراج.

.1د SPAN هدف

SPANد لاندې کارونو لپاره کارول کېږي:

- د Network Traffic څارنه

- Packet Capture
- د Network ستونزوTroubleshooting
- دTraffic Analysis
- دSecurity Monitoring

که Fa0/1د **Source Port**او Fa0/10د **Destination Port**په توګه تنظيم شي، د Traffic Fa0/1يوه کاپي Fa0/10ته لېږل کېږي.

2. Source Port

Source Portهغه Port دی چې Traffic ترې ځارل کېږي.

مثلاً:

Fa0/1

3. Destination Port

Destination Portهغه Port دی چې د Source Traffic کاپي ورته استول کېږي.

مثلاً:

Fa0/10

په دې Port کې د Packet Capture يا Monitoring وسيله نښلول کېږي.

4. SPAN Configuration

فرض کړئ:

- Source Port = Fa0/1
- Destination Port = Fa0/10

Configuration:

```
Switch> enable
Switch# configure terminal

Switch(config)# monitor session 1 source interface fa0/1
Switch(config)# monitor session 1 destination interface fa0/10
```

monitor session 1

د SPAN Session نمبر دی.

source interface fa0/1

دFa0/1 Traffic Source ټاکي.

destination interface fa0/10

دFa0/10 Traffic Destination ټاکي.

5. د Source لپاره RX اوTX

SPANکولی شي د Interface د Traffic مختلف لوري وڅاري.

RX

Received Traffic: يوازې

```
Switch(config)# monitor session 1 source interface fa0/1 rx
```

TX

Transmitted Traffic: يوازې

```
Switch(config)# monitor session 1 source interface fa0/1 tx
```

Both

دواړه لوري:

```
Switch(config)# monitor session 1 source interface fa0/1 both
```

6. د VLAN Traffic Monitoring

د یوه VLAN Traffic هم د SPAN له لارې Destination Port ته کاپي کېدای شي.

مثلاً: VLAN 10

```
Switch(config)# monitor session 1 source vlan 10
Switch(config)# monitor session 1 destination interface fa0/10
```

دلته د VLAN 10 Traffic د Destination Port Fa0/10 ته کاپي کېږي.

7. د SPAN Verification

د SPAN Session د کتلو لپاره:

```
Switch# show monitor
```

دا Command د SPAN Session معلومات ښکاره کوي.

8. د SPAN Configuration لرې کول

د Session د لرې کولو لپاره:

```
Switch(config)# no monitor session 1
```

د روټر بنسټیز Configuration او Router Basic Configuration

Router Basic Configuration هغه لومړني تنظیمات دي چې په Cisco Router کې د CLI له لارې ترسره کېږي، ځو روټر د شبکې لپاره مناسب نوم، امنیت، Interface IP Address او نور اړین تنظیمات ولري.

د Cisco IOS سره د کار لپاره باید د **CLI (Command-Line Interface)** له لارې Configuration ترسره شي. کتاب هم ټینګار کوي چې د Router او Switch د کار لپاره د CLI مهارت اړین دی.

1. Router ته د Privileged EXEC Mode ته داخلېدل

په پیل کې روټر عموماً په **User EXEC Mode** کې وي:

```
Router>
```

د Privileged EXEC Mode ته د تلو لپاره:

```
Router> enable
Router#
```

enable کمانډ د Privileged EXEC Mode ته داخلوي.

2. Global Configuration Mode ته داخلېدل

له Privileged EXEC Mode څخه د Configuration Mode ته د تلو لپاره:

```
Router# configure terminal
Router(config)#
```

یا لنډ شکل:

```
Router# conf t
```

په دې Mode کې د روټر عمومي Configuration ترسره کېږي.

3. د Router نوم ټاکل

د روټر د پېژندلو لپاره ورته مناسب **Hostname** ټاکل کېږي:

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

له دې وروسته د روټر Prompt له Router څخه R1 ته بدلېږي. د Cisco IOS په Configuration کې د hostname کمانډ کارول د کتاب په مثالونو کې هم لیدل کېږي.

4. د Privileged EXEC Password لپاره ټاکل

د Privileged EXEC Mode د خوندي کولو لپاره **enable secret** کارول کېږي:

```
R1(config)# enable secret Cisco123
```

enable secret د Privileged EXEC Mode لپاره Password ټاکي.

د کتاب له مخې، Cisco IOS د Password لپاره مختلف Hash/Encoding ډولونه هم ملاتړ کوي، او د enable secret کارول د enable password په پرتله د Password د خوندي کولو لپاره غوره انتخاب دی.

5. د Console Line لپارهPassword

د Console له لارې د Router د لاسرسي لپاره Password ټاکل کېدای شي:

```
R1(config)# line console 0
R1(config-line)# password Cisco123
R1(config-line)# login
R1(config-line)# exit
```

دلته:

- line console 0 ⟶ Console Line ته داخلېږي.
- password Cisco123 ⟶ Password ټاکي.
- login ⟶ ټاکل شوی Password د Login لپاره فعالوي.
- exit ⟶ له Console Configuration Mode څخه وځي.

6. د Router Interface ته IP Address ورکول

د Router Interface د شبکې سره د نښلولو لپاره IP Address او Subnet Mask ورکول کېږي.

مثال:

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
```

د Interface د فعالولو لپاره:

```
R1(config-if)# no shutdown
```

په دې توګه د Interface Configuration داسې کېدای شي:

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
```

د کتاب په Router Configuration مثالونو کې هم interface، ip address او no shutdown د Interface د تنظیم لپاره کارول شوي دي.

7. د Interface حالت کتل

د Router د Interface د IP Address او Status د کتلو لپاره:

```
R1# show ip interface brief
```

دا کمانډ د Interface مهم معلومات په لنډ شکل ښیي.

8. Running Configurationکتل

د Router اوسنی Configuration د کتلو لپاره:

```
R1# show running-config
```

Running-configهغه Configuration ده چې Router یې اوس مهال په RAM کې کاروي.

9. Configurationخوندي کول

که Configuration خوندي نه شي، د Router له Restart وروسته ممکن له منځه ولاړه شي. د Running Configuration د Startup Configuration ته د انتقال لپاره:

```
R1# copy running-config startup-config
```

یا:

```
R1# write memory
```

د کتاب له مخې، copy running-config startup-config د Configuration د Backup او Restore په پروسه کې هم کارول کېږي.

د Router Basic Configuration بشپړ مثال

```
Router> enable
Router# configure terminal

Router(config)# hostname R1

R1(config)# enable secret Cisco123

R1(config)# line console 0
R1(config-line)# password Cisco123
R1(config-line)# login
R1(config-line)# exit

R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit

R1(config)# end

R1# show ip interface brief
R1# show running-config
R1# copy running-config startup-config
```

مهمCommands

دنده	Command
Privileged EXEC Modeته داخلېدل	enable
Global Configuration Modeته تلل	configure terminal
د Router نوم ټاکل	hostname R1
د Privileged EXEC لپارهSecret Password	enable secret Cisco123
Console Lineته داخلېدل	line console 0
Console Passwordټاکل	password Cisco123
Console Loginفعالول	login
Interfaceته داخلېدل	interface gigabitethernet 0/0
IP Addressاو Subnet Mask ټاکل	ip address 192.168.1.1 255.255.255.0
Interfaceفعالول	no shutdown
د Interface حالت او IP معلومات کتل	show ip interface brief
اوسنی Configuration کتل	show running-config
Configurationخوندي کول	copy running-config startup-config

Routing Theoryد Routing نظریه

Routingهغه پروسه ده چې Router پرې ټاکي چې د IP Packet د Destination شبکې ته د رسېدو لپاره باید کومه لاره وکارول شي.
Routerد Packet د Forward کولو لپاره د **Routing Table**معلومات کاروي. که د Packet د Destination لپاره په Routing Table کې مناسبه Route موجوده نه وي، Router Packetردوي.

Routing Table

Routing Tableهغه جدول دی چې Router پکې د شبکې د مختلفو Destination Networks په اړه معلومات ساتي.

د CCNA 200-301 په Routing Table کې لاندې مهم اجزا شامل دي:

- **Routing Protocol Code**
- **Prefix**
- **Network Mask**
- **Next Hop**
- **Administrative Distance**
- **Metric**
- **Gateway of Last Resort**

Next Hop

Next Hopهغه Router یا IP Address دی چې Packet باید لومړی ورته ولېږل شي، څو د Destination شبکې پر لوري حرکت وکړي.

د مثال په توګه، که R3 د R1 له لارې یوې بلې شبکې ته رسېږي، د R3 په Routing Table کې د R1 Interface IP Address د **Next Hop**په توګه ثبتېدای شي.

Administrative Distance

Administrative Distance (AD)د Routing Information د اعتبار د ټاکلو لپاره کارېږي. که Router د یوې Destination شبکې لپاره له مختلفو Routing Sourcesڅخه Route ترلاسه کړي، Administrative Distanceد دې په ټاکلو کې مرسته کوي چې کوم Source ته لومړیتوب ورکړل شي.

Metric

Metricهغه ارزښت دی چې Routing Protocol یې د Route د غوره والي د ټاکلو لپاره کاروي. د Routing Protocol له مخې د Metric د محاسبې طریقه توپیر کولی شي.

Gateway of Last Resort

Gateway of Last Resortد هغه Traffic لپاره د لارې په توګه کارېږي چې Router یې د Destination لپاره مشخصه Route نه لري. دا عموماً د **Default Route**سره تړاو لري.

Static Routingثابت Routing

Static Routeهغه Route ده چې Network Administrator یې په لاسي ډول په Router کې Configuration کوي.

په Static Routing کې Router Route د Routing Protocol له لارې نه زده کوي؛ بلکې Administrator په مستقیم ډول د Destination شبکې لپاره Routeمشخصوي.

د CCNA 200-301 په موضوعاتو کې د IPv4 او IPv6 Static Routing لپاره لاندې ډولونه شامل دي:

1. Default Route

Default Routeهغه Route ده چې د هغو Destination Networks لپاره کارېږي چې په Routing Table کې ورته مشخصه Route موجوده نه وي.

په ساده ډول:

که ځانګړې Route پیدا نه شوه ⟶ Default Route

2. Network Route

Network Routeد یوې بشپړې شبکې لپاره Route ده.

مثلاً:

192.168.10.0/24

دا Route Router ته ښیي چې د 192.168.10.0/24شبکې ته د رسېدو لپاره کومه لاره وکاروي.

3. Host Route

Host Routeیوازې د یوه ځانګړې Host د IP Address لپاره Route ده.

د مثال په توګه:

192.168.10.10/32

دا Route یوازې د Host 192.168.10.10لپاره ده.

4. Floating Static Route

Floating Static Routeیوه اضافي Static Route ده چې د اصلي Route د ناکامېدو پر مهال د Backup په توګه کارول کېږي.

د دې لپاره د اصلي Route په پرتله لوړه **Administrative Distance**ټاکل کېږي، ځو تر هغه وخته Routing Table ته د اصلي Route په شتون کې لومړیتوب ورنه کړي.

Dynamic Routing

Dynamic Routingهغه Routing طریقه ده چې Router د **Routing Protocols**له لارې Routes زده کوي او د Routing Table معلومات په اتومات ډول جوړوي، بدلوي او تازه کوي.

د کتاب له مخې، Routing Protocolsد Routerد **Control Plane**له مهمو پروسو څخه دي Routing Protocols .د IP Routing Table ته Routes اضافه کوي، Routesلرې کوي او د اړتیا پر مهال یې بدلوي.

د Dynamic Routing مهم Routing Protocols چې کتاب یې یادوي:

- **OSPF**
- **EIGRP**
- **RIP**
- **BGP**

OSPF

OSPF (Open Shortest Path First)د Dynamic Routing یو مهم Protocol دی.

په Traditional Network کې OSPF د هر Router پر Control Plane کې کار کوي OSPF .د Routing معلوماتو پر بنسټ د Router Routing Table جوړوي او تازه کوي.

د CCNA 200-301 لپاره د **Single-Area OSPFv2**موضوع کې لاندې مفاهیم مهم دي:

- **Neighbor Adjacencies**
- **Point-to-Point**
- **Broadcast**
- **DR/BDR Selection**
- **Router ID**

Static Routingاو Dynamic Routing توپیر

Dynamic Routing	Static Routing	ګانګرتیا
د Routing Protocol له لارې	په لاسي ډول	Routeڅنګه زده کېږي؟
Protocolپې زده او تازه کوي	Administratorپې تنظیموي	Configuration
په اتومات ډول Route Update کولی شي	عموماً لاسي بدلون غواړي	د شبکې بدلون
Routing Protocolکاروي	اړتیا نه لري	Routing Protocol
OSPF, EIGRP, RIP, BGP	Static Route	مثال
Protocolد موجودو Routes له مخې انتخاب کوي	Floating Static Routeکارېدلی شي	Backup Route

لنډه پایله

Routingد Packet د Destination پر لوري د مناسبې لارې ټاکلو پروسه ده Router .د دې کار لپاره **Routing Table**کاروي Routes .په عمومي ډول د **Static Routing**یا **Dynamic Routing**له لارې Routing Table ته داخلېږي Static Routes Administrator .په لاسي ډول تنظیموي، خو Dynamic Routingد OSPF، EIGRP ، RIPاو BGP په څېر Routing Protocols له لارې Routes زده کوي او Routing Table تازه کوي.

Static Routing and Dynamic Routing Configuration

په دې برخه کې به **Static Routing Configuration**او **Dynamic Routing Configuration**په Cisco IOS کې عملي ډول تنظیم کړو. د ورکړل شوي کتاب له مخې، Routerد Packet د Forward کولو لپاره Routing Table ته اړتیا لري؛ Dynamic Routing Protocols لکه **OSPF**د Routing Table معلومات جوړوي او تازه کوي.

مهمه یادونه :ستاسې ورکړل شوی **Volume 2**د Static Routing او Dynamic Routing بشپړ Configuration فصل نه لري. د Static Route لپاره ip route کمانډ په کتاب کې ثبت شوی، او د OSPF Configuration یو مثال هم موجود دی؛ نو لاندې Configuration یوازې هغه برخې پوښي چې له فایل څخه یې ملاتړ کېږي.

Static Routing Configuration

Static Routeهغه Route ده چې Administrator یې په لاسي ډول Router ته Configuration کوي.

د Cisco IOS په Router کې د Static Route لپاره د Configuration Command ip routeکارول کېږي. کتاب هم ځرګندوي چې IOS د ip routeله لارې Configureشوې Static Route ته عموماً **Administrative Distance = 1**ورکوي.

د Static Route عمومي Syntax

```
Router(config)# ip route destination-network subnet-mask next-hop-ip
```

مثال:

```
R1(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2
```

دلته:

- 192.168.2.0 ⟶ Destination Network
- 255.255.255.0 ⟶ Subnet Mask
- 10.0.0.2 ⟶ Next-Hop Router

یعنې R1 ته ویل کېږي چې د **192.168.2.0/24**شبکې ته د رسېدو لپاره Packet د Next-Hop **10.0.0.2**ته ولېږي.

Static Default Route

Default Routeد هغو Destination Networks لپاره کارېږي چې Router ورته مشخصه Route ونه لري.

د Default Route لپاره Destination او Mask دواړه 0.0.0.0وي:

```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

په Routing Table کې د Default Route د 0.0.0.0/0په توګه ځرګندېږي. د کتاب په DHCP مثال کې هم Default Route د 0.0.0.0/0په بڼه ښودل شوې ده.

Static Route Verification

د Static Routes د کتلو لپاره:

```
R1# show ip route static
```

د کتاب په مثال کې همدا کمانډ کارول شوی:

```
R1# show ip route static
```

او د Default Route مثال:

```
S* 0.0.0.0/0 [254/0] via 192.0.2.1
```

Dynamic Routing Configuration

Dynamic Routingکې Router د Routing Protocol له لارې Routes زده کوي او Routing Table ته یې اضافه، حذف یا Update کوي.

د کتاب له مخې، **OSPF**، **EIGRP**، **RIP**او **BGP** د Control Plane له مهمو Routing Protocols څخه دي.

په CCNA کې د Dynamic Routing لپاره **OSPF**مهم مثال دی.

OSPF Configuration

د کتاب په موجود Configuration Example کې د Router پر Interface باندې OSPF فعال شوی:

```
interface GigabitEthernet0/1/0
ip address 10.1.12.1 255.255.255.0
ip ospf 1 area 11
!
```

```
router ospf 1
router-id 1.1.1.1
```

د Configuration تشریح

```
interface GigabitEthernet0/1/0
```

Routerته د مشخص Interface Configuration Mode ته داخلېږي.

```
ip address 10.1.12.1 255.255.255.0
```

Interfaceته IPv4 Address او Subnet Mask ورکوي.

```
ip ospf 1 area 11
```

په دې Interface باندې **OSPF Process 1**فعالوي او Interface يې **OSPF Area 11**ته داخلوي.

```
router ospf 1
```

د OSPF Routing Process Configuration Mode فعالوي.

```
router-id 1.1.1.1
```

د Router لپاره OSPF Router ID ټاکي.

Staticاو Dynamic Routing Configuration پرتله

Dynamic Routing	Static Routing	ګانګرتیا
د Routing Protocol له لارې	لاسي	Configuration
router ospf / ip ospf	ip route	اصليCommand
Routing Protocolيې Update کوي	Administratorيې بدلوي	Route Update
Protocolيې زده کوي	په Static Route کې مشخصېږي	Next-Hop
OSPF	ip route ...	مثال
Protocol Routesاضافه/بدلوي	Static Routeاضافه کوي	Routing Table

د کتاب له مخې، د Dynamic Routing په حالت کې OSPF د Router د Control Plane برخه ده او د IP Routing Table ته Routes **اضافه، حذف او بدلوي**.

مهمCommands

Static Routing

```
configure terminal
ip route 192.168.2.0 255.255.255.0 10.0.0.2
end
show ip route static
```

OSPF Dynamic Routing

```
configure terminal
interface GigabitEthernet0/1/0
ip address 10.1.12.1 255.255.255.0
ip ospf 1 area 11
exit
router ospf 1
router-id 1.1.1.1
end
```

مهم توپیر

Static Routing:

Administrator ⟶ Route ⟶ Routing Table

Dynamic Routing:

Routing Protocol ⟶ Route Information ⟶ Routing Table

په همدې اساس، Static Routingکې Administrator Route په لاسي ډول جوړوي، خو Dynamic Routing کې OSPF په ځېر د Routing Protocol Routing Tableمعلومات په اتومات ډول جوړوي او تازه کوي.

RIP – Routing Information Protocol

RIP (Routing Information Protocol) د **Dynamic Routing Protocol** له ډلې څخه دی. د کتاب له مخې، RIP د Router د **Control Plane** له Routing Protocols څخه یو دی. Control Plane د Routing Table معلومات جوړوي، بدلوي او تازه کوي، څو Router وکولای شي د Packet د Forward کولو لپاره مناسبې لارې وکاروي.

RIP څه کوي؟

RIP د شبکې د مختلفو برخو Routes د Routing Protocol Update له لارې Router ته رسوي. Router د RIP له لارې Routes زده کوي او په Routing Table کې یې کاروي.

د مثال په توګه، که **R1** او **R2** سره وصل وي او R2 د یوې بلې شبکې Route ولري، RIP کولای شي د R2 له لارې دغه Route R1 ته ور وپېژني. R1 کولای شي د RIP له لارې د **Network B** په اړه Routing Information ترلاسه کړي.

RIPv2

د کتاب په موجودو مطالبو کې **RIPv2** هم یاد شوی دی. RIPv2 د **UDP** څخه د Transport لپاره استفاده کوي او د **UDP Port 520** کاروي.

د RIPv2 پیغامونو لپاره:

Protocol: UDP

Port: 520

Destination: 224.0.0.9

د کتاب له مخې، RIPv2 د Routing Updates لپاره **224.0.0.9** Multicast Address کاروي.

RIP او Control Plane

RIP د Router د **Control Plane** برخه ده. Control Plane د Routing Table جوړولو او تازه کولو دنده ترسره کوي.

د کتاب له مخې، Routing Protocols لکه **OSPF**، **EIGRP**، **RIP** او **BGP** د Control Plane مهم Protocols دي.

RIP او ACL

د RIP لپاره یو مهم Troubleshooting ټکی دا دی چې که په Router باندې **Inbound ACL** نصب وي او د RIP Update پیغامونه اجازه ونه لري، Router ممکن له بل Router څخه RIP Routes زده نه کړي.

د کتاب په مثال کې، R2 د RIP Updates لېږي، خو R1 باندې ACL د RIP پیغامونه د **Implicit Deny** له امله ردوي؛ پایله دا وي چې R1 له R2 څخه Routes نه زده کوي.

RIPv2 د ACL په وخت کې د لاندې معلوماتو له مخې پېژندل کېدای شي:

Subnetting د شبکې وېشل ——

Subnetting هغه پروسه ده چې یوه IP Network په کوچنیو **Subnets** وېشي. د Subnetting لپاره د **IP Address** ترڅنګ **Subnet Mask** کارول کېږي.

د کتاب له مخې، Host د خپل **IP Address** او **Subnet Mask** په وسیله محاسبه کوي چې کوم IP Addresses د هغه په **هماغه Subnet** کې دي او کوم Addresses په نورو Subnets کې دي.

Subnet Mask

Subnet Mask د IP Address هغه برخه مشخصوي چې د Network/Subnet لپاره کارېږي او هغه برخه مشخصوي چې د Host لپاره پاتې کېږي.

د مثال په توګه:

IP Address: 192.168.1.172

Subnet Mask: 255.255.255.0

په Prefix Notation کې:

192.168.1.172/24

دلته /24 د Subnet Mask Prefix Length ښيي.

Subnet ID

Subnet ID د Subnet د پېژندلو لپاره کارېږي. DHCP Server هم د Subnet ID او Mask پر اساس پوهېږي چې د یوې Subnet ټول Addresses کوم دي.

د مثال په توګه:

Subnet: 192.168.1.0/24

په دې Subnet کې د Host IP Address یوه بېلګه:

192.168.1.172

د کتاب د Windows مثال هم 192.168.1.172له Subnet Mask 255.255.255.0سره ښيي.

Hostاو Subnet اړيکه

کله چې Host غواړي يو Packet ولېږي، لومړی د خپل **IP Address**او **Subnet Mask**پر اساس معلوموي چې Destination Address په خپل Subnet کې دی او که له Subnet څخه بهر دی.

که Destination په هماغه Subnet کې وي، Hostکوالی شي مستقيم ورته Packet ولېږي.

که Destination له Subnet څخه بهر وي، Host Packetخپل **Default Gateway**ته استوي.

مثال

Host IP: 192.168.1.172

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

د Host او Default Gateway Subnet بايد يو شان وي؛ ځکه دواړه بايد د Subnet حدود په يو ډول محاسبه کړي.

DHCPاوSubnetting

DHCP Serverعموماً د هر Subnet لپاره جلا معلومات ساتي. د DHCP Pool د جوړولو پر مهال **Subnet ID**او **Mask** مشخصېږي:

network 172.16.1.0 255.255.255.0

يا د Prefix Length په شکل:

network 172.16.2.0 /24

DHCP Serverله Subnet ID او Mask څخه د دې لپاره استفاده کوي چې د Subnet ټول Addresses وېښتني Server .د **Subnet ID**او **Subnet Broadcast** **Address**په څېر Addresses Host ته نه ورکوي.

مهم اصطلاحات

اصطلاح	معنا
IP Address	د Host شبکه‌ییزAddress
Subnet Mask	د Network او Host برخې معلوموي
Prefix Length	د Mask لنډه بڼه، لکه 24/
Subnet ID	د Subnet پېژندونکیNetwork Address
Default Gateway	هغه Router چې له Subnet څخه بهر Traffic ته کارېږي
Host Address	په Subnet کې د يوه Device لپارهAddress

EIGRP – Enhanced Interior Gateway Routing Protocol

EIGRP (Enhanced Interior Gateway Routing Protocol)د **Dynamic Routing Protocol**له ډلې څخه دی. د کتاب له مخې، EIGRPد Router د **Control Plane**له مهمو Routing Protocols څخه شمېرل کېږي. د Control Plane Routing Table معلومات جوړوي، بدلوي او تازه کوي، څو Router وکولای شي د Packet د Forward کولو لپاره مناسبې لارې وکاروي.

Control PlaneاوEIGRP

په Traditional Network کې Routing Protocols د **Distributed Control Plane**په بڼه کار کوي؛ يعنې هر Router خپل Routing Protocol Process لري.

EIGRPهم د همدې Routing Protocols له ډلې څخه دی، لکه:

- **OSPF**
- **EIGRP**
- **RIP**
- **BGP**

دا Protocols د Routing Information په کارولو سره د Router د Routing Table په جوړولو او تازه کولو کې مرسته کوي.

EIGRP د ACL په حالت کې

د کتاب له مخې، **EIGRP د TCP یا UDP Transport Protocol نه کاروي**. له همدې امله، د EIGRP پیغامونه د ACL په وسیله د TCP/UDP Port پر بنسټ نه Match کېږي؛ بلکې د Cisco IOS د **eigrp** ځانګړی ACL Protocol Keyword وړاندې کوي.

د EIGRP لپاره مهم معلومات:

EIGRP	ځانګړتیا
Enhanced Interior Gateway Routing Protocol	بشپړ نوم
Dynamic Routing Protocol	ډول
Control Plane	Plane
TCP/UDP نه کاروي	Transport Protocol
224.0.0.10	Destination Multicast Address
eigrp	ACL Keyword

د EIGRP د ACL اجازه

که Inbound ACL د EIGRP Routing Updates مخه ونیسي، Routerممکن د EIGRP له لارې Routing Information ترلاسه نه کړي. د EIGRP پیغامونو د اجازه ورکولو لپاره:

```
R1(config)# ip access-list extended RoutingProtocolExample
R1(config-ext-nacl)# permit eigrp any any
```

د کتاب په مثال کې هم permit eigrp any any د EIGRP پیغامونو د اجازه ورکولو لپاره کارول شوی.

یادونه : د ورکړل شوي **CCNA 200-301 Volume 2** کتاب له مخې د EIGRP بشپړ Configuration او Verification نه دی تشریح شوی؛ کتاب په ځانګړي ډول EIGRP د Control Plane Protocol او د ACL اړوند موضوعاتو کې یادوي. حتی کتاب ځرګندوي چې د CCNA 200-301 اصلي Exam Topics کې د EIGRP د **Configuration and Verification** موضوع نه ده شامله شوې.

Wildcard Mask – Summarization – VLSM

د ورکړل شوي **CCNA 200-301 Official Cert Guide, Volume 2** له مخې، دا درې اصطلاحات په یوه کچه نه دي تشریح شوي **Wildcard Mask**. په تفصیل سره د IPv4 ACLs لپاره تشریح شوی، خو **Summarization** او **VLSM** په دې Volume 2 کې د مستقلو موضوعاتو په توګه بشپړ نه دي تشریح شوي. نو لاندې معلومات یوازې د کتاب له موجودې محتوا سره سم وړاندې کېږي.

1. Wildcard Mask

Wildcard Mask د Cisco IOS په ACL Commands کې کارېږي. دا **Subnet Mask نه دی**؛ بلکې Router ته وایي چې د IP Address کومې برخې باید پرتله کړي او کومې برخې باید له پامه وغورځوي.

د Wildcard Mask دوه اساسي قواعد:

- Router ⟶ **0** باید دغه برخه عادي ډول Compare کړي.
- Router ⟶ **255** باید دغه برخه Ignore کړي.

مشهور Wildcard Masks

دنده	Wildcard Mask
وروستی Octet Ignore کوي	0.0.0.255
وروستي دوه Octets Ignore کوي	0.0.255.255
وروستي درې Octets Ignore کوي	0.255.255.255

د Subnet لپاره Wildcard Mask

د یوې Subnet د Match کولو لپاره:

Wildcard Mask = 255.255.255.255 – Subnet Mask

مثلاً:

Subnet Mask:

255.255.255.0

Wildcard Mask:
0.0.0.255

نو د 192.168.1.0/24لپاره ACL داسې کېدای شي:
access-list 1 permit 192.168.1.0 0.0.0.255
دا د 192.168.1.0څخه تر 192.168.1.255پورې Address Range Match کوي.

Summarization

Summarizationيا **Route Summarization**د څو کوچنيو Network Routes د يوې لويې Summary Route په توګه د بيانولو مفهوم دی.
د ورکړل شوي کتاب په Wildcard Mask برخه کې **Summary Route**د څو Subnets د يوځای کولو د مثال په توګه ياد شوی، خو د **Route Summarization**بشپړ Configuration او تفصيلي تشريح په دې Volume 2 کې نه ده وړاندې شوې.
د مفهوم ساده مثال:
192.168.0.0/24
192.168.1.0/24
192.168.2.0/24
192.168.3.0/24
دا څو شبکې په مناسب حالت کې د يوې لويې Summary Route په وسيله بيانېدای شي:
192.168.0.0/22
هدف :د څو Routes پر ځای د يوې Summary Route استعمالول، څو Routing Information ساده او منظم شي.
يادونه :پورته مثال د Summarization د مفهوم د روښانتيا لپاره دی؛ د ورکړل شوي Volume 2 له مخې يې بشپړ Routing Configuration نه دی وړاندې شوی.

VLSM

VLSM (Variable Length Subnet Mask)د Subnetting هغه مفهوم دی چې په يوه Network کې د مختلفو Subnets لپاره مختلف Prefix Lengths يا Subnet Masksکارول کېږي.
د مثال په ډول، د يوې شبکې لپاره ممکن دا ډول Subnets موجود وي:
192.168.1.0/24
192.168.2.0/25
192.168.2.128/26
دلتهPrefix Length ونه يو شان نه دي:
/24
/25
/26
له همدې امله ورته **Variable Length Subnet Mask**ويل کېږي.
خو مهمه خبره :د ورکړل شوي **CCNA 200-301 Official Cert Guide, Volume 2**په موجوده محتوا کې VLSM د يوه مستقل فصل يا بشپړ تشريح شوي Topicپه توګه نه دی وړاندې شوی؛ نو د کتاب له مخې يې له دې څخه زيات جزئيات نه شم ورزياتولی.
د دې Volume 2 له مخې تر ټولو تفصيلي موضوع يې Wildcard Mask ده.

OSPF – Open Shortest Path First

OSPF (Open Shortest Path First)د **Dynamic Routing Protocol**له ډلې څخه دی. د CCNA کتاب له مخې، OSPFد Router د **Control Plane**يو مهم Protocolدی OSPF .په هر Router کې کار کوي او د Routing Table د جوړولو، Routesد اضافه کولو، حذف کولو او بدلولو لپاره Routing Information کاروي.

OSPFپه شبکه کې

په Traditional Network کې هر Router خپل OSPF Process لري Routers .د OSPF پيغامونو له لارې له يو بل سره Routing Information شريکوي.

هر Router د OSPF له لارې ترلاسه شوې معلومات کاروي، څو خپل **IP Routing Table**جوړ او تازه کړي.

OSPF Neighbor

هغه Routers چې د OSPF له لارې له یو بل سره Routing Information تبادله کوي، **OSPF Neighbors** بلل کېږي.

د مثال په توګه، د MPLS شبکې په یوه ډیزاین کې Customer Edge (**CE**) Router د Service Provider د **PE Router** سره OSPF Neighbor Relationship جوړوي، خو له نورو CE Routers سره مستقیم OSPF Neighbor Relationship نه جوړوي.

OSPF Area

OSPF شبکه په **Areas** وېشلای شي. د OSPF په ډیزاین کې **Area 0** د **Backbone Area** په توګه کارول کېږي.

د MPLS VPN په ځانګړي ډیزاین کې د **OSPF Super Backbone** مفهوم هم شته. په دې حالت کې MPLS PE Routers د Super Backbone په توګه کار کوي، او PE-CE Link د Backbone Area یا Non-Backbone Area برخه کېدای شي.

OSPF Hello Messages

OSPF د Neighbor د پېژندلو او د Neighbor Relationship د ساتلو لپاره **Hello Messages** کاروي.

د کتاب د Debug مثال کې OSPF Hello پیغام:

```
OSPF-1 HELLO Gi0/1:
Send hello to 224.0.0.5 area 0
```

ښودل شوی دی.

په دې مثال کې:

- **OSPF-1** ⟶ OSPF Process
- **Gi0/1** ⟶ Interface
- **224.0.0.5** ⟶ د OSPF Hello لپاره Multicast Address
- **Area 0** ⟶ OSPF Area

OSPF Configuration

د کتاب په Configuration مثال کې OSPF په Interface باندې داسې فعال شوی:

```
interface GigabitEthernet0/1/0
ip address 10.1.12.1 255.255.255.0
ip ospf 1 area 11
!
router ospf 1
router-id 1.1.1.1
```

د Configuration تشریح

```
ip ospf 1 area 11
```

په Interface باندې **OSPF Process 1** فعالوي او Interface د **Area 11** برخه ګرځوي.

```
router ospf 1
```

د Configuration **OSPF Process 1** ته داخلېږي.

```
router-id 1.1.1.1
```

د Router لپاره **OSPF Router ID** ټاکي.

OSPF او Control Plane

د Router د **Data Plane** لپاره Routing Table اړینه ده. OSPF د Control Plane په توګه د Routing Table معلومات برابروي.

```
OSPF
↓
Routing Information
↓
IP Routing Table
↓
Data Plane
↓
Packet Forwarding
```

که Routing Table کې د Packet د Destination لپاره مناسبه Route موجوده نه وي، Router Packetردوي.

OSPFپه CCNA کې مهم ټکي

د ورکړل شوي کتاب له محتوا سره سم، د OSPF اړوند مهم مفاهیم دا دي:

- **OSPF Routing Protocol**
- **OSPF Neighbor Relationship**
- **OSPF Hello Messages**
- **OSPF Area**
- **Area 0 / Backbone Area**
- **OSPF Router ID**
- **OSPF Process**
- **OSPF Super Backbone**
- **PE-CE OSPF Relationship**
- **OSPF اوRouting Table**

یادونه :ستاسې د ورکړل شوي **CCNA 200-301 Official Cert Guide, Volume 2**په دې برخه کې OSPF په ښه ډول تشریح شوی، خو د OSPFبشپړ عمومي Configuration فصل پکې نشته؛ نو پورته Configuration یوازې د کتاب له موجود مثال څخه اخیستل شوې ده.

OSPF Configuration

د ورکړل شوي **CCNA 200-301 Official Cert Guide, Volume 2**له مخې، د OSPF Configuration نمونه داسې ده. په دې مثال کې Router ته IP Addressورکول کېږي، OSPFپه Interface کې فعالېږي، Areaټاکل کېږي او Router ID تنظیمېږي.

OSPF Configuration

```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# ip ospf 1 area 11
R1(config-if)# exit

R1(config)# interface GigabitEthernet0/1/0
R1(config-if)# ip address 10.1.12.1 255.255.255.0
R1(config-if)# ip ospf 1 area 11
R1(config-if)# exit

R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
```

د Commands معنا

`interface GigabitEthernet0/0`

د Router ټاکلي Interface ته داخلېږي.

`ip address 10.1.1.1 255.255.255.0`

Interfaceته IPv4 Address او Subnet Mask ټاکي.

`ip ospf 1 area 11`

په Interface باندې **OSPF Process 1**فعالوي او Interface د **Area 11**برخه ګرځوي.

`router ospf 1`

د Configuration Mode **OSPF Process 1**ته داخلېږي.

`router-id 1.1.1.1`

د OSPF لپاره Router ID ټاکي.

د دووRouterونو سادهConfiguration

R1

```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# ip ospf 1 area 11
R1(config-if)# exit

R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
```

R2

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip address 10.1.1.2 255.255.255.0
R2(config-if)# ip ospf 1 area 11
R2(config-if)# exit

R2(config)# router ospf 1
R2(config-router)# router-id 2.2.2.2
```

د کتاب د OSPF مثالونو له مخې، OSPFپه Router کې د Control Plane برخه ده او د Routing Table د جوړولو او تازه کولو لپاره کار کوي.

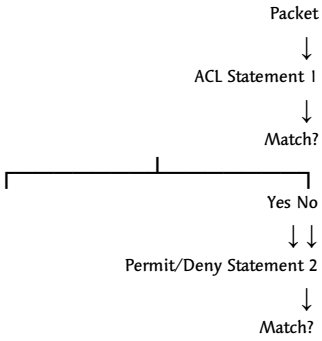
ACL — Access Control List

ACL (Access Control List)د Router یا نورو Network Devices لپاره د **Traffic Filtering**یوه وسیله ده .د ACL د Packet د ځانګړو معلوماتو پر بنسټ پربکړه کوي چې Packet ته باید **اجازه (Permit)** ورکړل شي او که **مخنیوی (Deny)** ترې وشي. د کتاب له مخې، ACLپه Router کې د Packet Flow د کنټرول لپاره کارېږي.

ACLڅنګه کار کوي؟

ACLد څو **ACE (Access Control Entry)**کرښو څخه جوړه وي. هره ACE د ACL یوه کرښه ده چې د Traffic د Match کولو شرایط او Action مشخصوي.

د ACL عمومي منطق:



ACLد Statements له پورته څخه ښکته په ترتیب سره ګوري. کله چې Packet له یوې Statement سره Match شي، Routerنورې Statements نه ګوري. دې ته **First-Match Logic**وایل کېږي.

Permitاو Deny

ACLد Match وروسته دوه اصلي Actions لري:

- Packet ⟶ **permit**ته اجازه ورکول کېږي.
- Packet ⟶ **deny**رد کېږي.

د ACL په پای کې یو **Implicit Deny All**موجود وي. یعنې که Packet له هېڅ Configured Statement سره Match نه شي، په پای کې رد کېږي.

له همدې امله، که غواړو نور ټول Traffic اجازه ولري، Explicit Permit Statementورزیاتولای شو:

```
access-list 1 permit any
```

د IPv4 ACL ډولونه

د کتاب له مخې IPv4 ACLs په دوو مهمو معیارونو وېشل کېږي:

1. Standard ACL

Standard ACLیوازې د **Source IP Address**پر اساس Packet Match کوي.

مثال:

```
access-list 1 permit 10.1.1.0 0.0.0.255
```

2. Extended ACL

Extended ACLد Standard ACL په پرتله ډېر معلومات Match کولای شي، لکه:

- Protocol
- Source IP Address
- Destination IP Address
- Source Port
- Destination Port

مثال:

```
access-list 101 permit tcp host 10.1.1.1 10.1.2.0 0.0.0.255 eq www
```

Named ACLاوNumbered

ACLsد نوم یا Number له مخې هم وېشل کېږي:

Numbered ACL

ACLد Number په وسیله پېژندل کېږي.

د Standard Numbered ACL لپاره:

```
1–99
1300–1999
```

د Extended Numbered ACL لپاره:

```
100–199
2000–2699
```

Named ACL

ACLد Number پر ځای د Name له لارې پېژندل کېږي.

د مثال په توګه:

```
ip access-list standard MY_ACL
```

یا:

```
ip access-list extended MY_ACL
```

ACLپه Interface کې فعالول

ACLیوازې د جوړولو په صورت کې Traffic نه Filter کوي؛ باید په مناسب Interface باندې هم فعال شي.

د Interface لپاره:

```
ip access-group {number | name}{in | out}
```

مثال:

```
interface Serial0
ip access-group 101 in
```

دلته 101 ACL د Serial0 Interface په **Inbound** Directionکې فعال شوی.

Outboundاو Inbound

Inbound ACL:

Packetد Interface له لارې Router ته له داخلېدو وروسته ACL پرې تطبیقېږي.

Outbound ACL:

Router Packet Routeکوي، بیا د Interface له لارې د وتلو پر مهال ACL پرې تطبیقېږي.

Wildcard Mask

ACLد IP Address د Match کولو لپاره **Wildcard Mask**کاروي.

د Wildcard Mask عمومي منطق:

- ۰دا برخه بايد Match شي. ⟵
- ۲۵۵دا برخه Ignore کېږي. ⟵

د مثال په توګه:

192.168.1.0 0.0.0.255

دا د Subnet Addresses Match 192.168.1.0کوي.

ACL Verification

د IPv4 ACLs د کتلو لپاره:

show ip access-lists

يا:

show access-lists

show ip access-listsد IPv4 ACLs معلومات ښيي، او show access-listsد IPv4 ترڅنګ د نورو ACL ډولونو معلومات هم ښودلی شي.

د Interface پر ACL د کتلو لپاره:

show ip interface

دا Command ښيي چې په Interface باندې کوم ACL او په کوم Direction کې فعال دی.

د ACL ساده مثال

R1(config)# access-list 1 permit 10.1.1.1

R1(config)# interface Serial0/0/1

R1(config-if)# ip access-group 1 in

په دې Configuration کې ۱ ACL د Source IP Address ۱۰.۱.۱.۱ته اجازه ورکوي او ACL د Interface Serial0/0/1 په Direction په **Inbound**کې فعالېږي.

لنډه پايله

ACL (Access Control List)د Network Traffic د کنټرول لپاره کارېږي. د Packet معلومات Match کوي او بيا د **permit**يا **deny**پربکړه کوي IPv4 . ACLsپه **Standard**او **Extended**ډولونو وېشل کېږي او د **Numbered**يا **Named**په بڼه Configuration کېدای شي. د ACL **First-Match Logic**له مخې کار کوي او که Packet له هېڅ Statement سره Match نه شي، **Implicit Deny**پرې تطبيقېږي.

NAT — Network Address Translation

NAT (Network Address Translation)هغه ميکانيزم دی چې د **Private IP Address**او **Public/Globally Routable IP Address**ترمنځ Translation ترسره کوي. د NAT له لارې هغه Hosts چې Private IP Addresses لري، کولای شي له Internet سره اړيکه ونيسي.

NATولې کارول کېږي؟

د IPv4 Address Space د محدوديت له امله Private IP Addresses په داخلي شبکو کې کارول کېږي. NAT بيا دغه Private Addresses د Internet پر لوري د تګ پر مهال په Public/Registered Addresses بدلوي.

مثال:

Private Network

10.1.1.1

|

| NAT

↓

Public Address

200.1.1.1

|

↓

Internet

کله چې Packet له داخلي شبکې څخه Internet ته وځي، NATد **Source IP Address** Packet بدلوي. کله چې Reply ښېرته راځي، NAT Destination Addressښېرته داخلي Address ته اړوي.

د NAT مهم اصطلاحات

Inside Local

د داخلي Host اصلي Private IP Address ته **Inside Local Address**ويل کېږي.

مثال:

10.1.1.1

Inside Global

هغه Public/Registered IP Address چې NAT يې د Inside Host د استازيتوب لپاره کاروي، **Inside Global Address**بلل کېږي.

مثال:

200.1.1.1

د کتاب په مثال کې:

Inside Local: 10.1.1.1

Inside Global: 200.1.1.1

Outside Local

د NAT د داخلي شبکې له لېدلوري د Outside Host Address ته **Outside Local**ويل کېږي.

Outside Global

د Outside Host واقعي Globally Routable Address/ته **Outside Global**ويل کېږي.

د NAT مهم ډولونه

په کتاب کې د NAT درې مهم ډولونه تشريح شوي دي:

1. Static NAT

Static NATد Inside Local او Inside Global Address ترمنځ **One-to-One Mapping**جوړوي.

مثال:

10.1.1.1 ↔ 200.1.1.1

10.1.1.2 ↔ 200.1.1.2

Static Mappingپه NAT Table کې د Timeout له امله نه حذف کېږي.

2. Dynamic NAT

Dynamic NATد Private Addressesد لپاره د Public IP Addresses له يوه **Pool**څخه Address اخلي.

مثال:

Private:

10.1.1.1

10.1.1.2

NAT Pool:

200.1.1.1

200.1.1.2

کله چې Inside Host Traffic توليد کړي، Routerد Pool څخه يو موجود Public Address ورته اختصاصوي.

3. NAT Overload / PAT

NAT Overloadچې **PAT (Port Address Translation)**هم ورته ويل کېږي، څو مختلف Inside Hosts ته اجازه ورکوي چې د يوه Public IP Address له لارې اړيکه ونيسي.

PATد IP Address ترڅنګ **Port Numbers**هم کاروي، نو څو مختلف Connections د يوه Public IP Address له لارې جلا پېژندل کېږي.

مثال:

10.1.1.1:49712 ┐

200.1.1.249 ── Internet ┤

10.1.1.2:49713 ┘

په دې حالت کې مختلف Inside Hosts/Connections د Port Numbers له لارې جلا کېږي.

NAT Configuration کې مهمCommands

Interface د Inside په توګه

```
interface GigabitEthernet0/0
ip nat inside
```

Interface د Outside په توګه

```
interface Serial0/0/0
ip nat outside
```

د ip nat inside اوip nat outside Commands Router ته مشخصوي چې کوم Interface د NAT د Inside او کوم د Outside شبکې برخه ده.

Static NAT

```
ip nat inside source static 10.1.1.1 200.1.1.1
```

دا د 10.1.1.1 او 200.1.1.1ترمنځ Static One-to-One Mapping جوړوي.

Dynamic NAT

Dynamic NATد ACL او NAT Pool څخه استفاده کوي:

```
ip nat inside source list 1 pool fred
```

دلته ACL مشخصوي چې کوم Inside Local Addresses بايد NAT شي، او pool fred د Inside Global Addresses سرچينه ده.

PAT

د کتاب مثال:

```
ip nat inside source list 1 interface Serial0/0/0 overload
```

دلته overload د PAT فعالولو لپاره مهم دی.

NAT Verification

د NAT Translation Table د کتلو لپاره:

```
show ip nat translations
R1(config)# interface GigabitEthernet0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# ip nat inside
R1(config-if)# no shutdown
R1(config-if)# exit

R1(config)# interface GigabitEthernet0/1
R1(config-if)# ip address 200.1.1.1 255.255.255.252
R1(config-if)# ip nat outside
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)# ip nat inside source list 1 interface GigabitEthernet0/1 overload
```

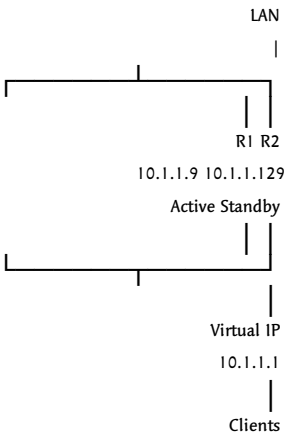
HSRP – Hot Standby Router Protocol

HSRP (Hot Standby Router Protocol) د **FHRP (First Hop Redundancy Protocol)** له دلې څخه دی HSRP .دوه یا زیات Routers ته اجازه ورکوي چې په یوه Subnet کې د **Default Gateway** دنده شریکه کړي. یو Router د **Active** په توګه کار کوي او بل Router د **Standby** په توګه انتظار کوي؛ که Active Routerناکام شي، Standby Router د Default Gateway دنده اخلي.

HSRP څنګه کار کوي؟

HSRP د Hosts لپاره یو **Virtual IP Address** جوړوي Hosts .د خپل Default Gateway په توګه د Router اصلي IP Address نه، بلکې همدا **Virtual IP Address** کاروي.

مثال:



د Host Default Gateway:

10.1.1.1

که **R1**ناکام شي، **R2**د HSRP Active Router رول اخلي، او Hosts خپل Default Gateway نه بدلوي.

HSRPمهم اصطلاحات

اصطلاح	معنا
Active Router	اوس مهال د Gateway اصلي دنده ترسره کوي
Standby Router	د Active Router د ناکامۍ په صورت کې د takeover لپاره انتظار کوي
Virtual IP Address	هغه IP چې Hosts يې Default Gateway په توګه کاروي
Virtual MAC Address	HSRP Virtual MAC Address
HSRP Group	هغه Group چې HSRP Routers پکې يو بل پېژني
Priority	د Active Router د انتخاب لپاره کارېدونکی ارزښت

HSRP Priority

په HSRP کې د **Priority**له مخې Active Router ټاکل کېږي. د کتاب په مثال کې:

R1 Priority = 110

R2 Priority = 100

نو R1 د لوړ Priority له امله **Active**او R2 **Standby** کېږي. د 100 HSRP Default Priority ده.

HSRP Configuration Example

د کتاب Configuration Example کې دواړه Routers د **Group 1**او 10.1.1.1 Virtual IP استعمالوي.

R1 ── Active Router

```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# ip address 10.1.1.9 255.255.255.0
R1(config-if)# standby version 2
R1(config-if)# standby 1 ip 10.1.1.1
R1(config-if)# standby 1 priority 110
R1(config-if)# standby 1 name HSRP-group-for-book
```

R2 ── Standby Router

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip address 10.1.1.129 255.255.255.0
R2(config-if)# standby version 2
R2(config-if)# standby 1 ip 10.1.1.1
R2(config-if)# standby 1 name HSRP-group-for-book
```

د Configuration مهمه برخه

standby 1 ip 10.1.1.1

دا د **Group 1** HSRP لپاره 10.1.1.1 Virtual IP Address ټاکي. همدا IP Address Hosts د Default Gateway په توګه کاروي.

standby 1 priority 110

R1ته 110 Priority ورکوي. ځکه چې 100 R2 Default Priority لري، R1د Active Router لپاره لوړ Priority لري.

standby version 2

HSRP Version 2فعالوي. د يوه HSRP Group ټول Routers بايد د HSRP يو شان Version استعمال کړي.

HSRP Verification

د HSRP لنډ Status لپاره:

R1# show standby brief

د بشپړ معلوماتو لپاره:

R1# show standby

د مثالVerification

R1# show standby brief

Interface Grp Pri P State Active Standby Virtual IP

Gi0/0 1 110 Active local 10.1.1.129 10.1.1.1

R1دلته **Active**دی، R2دی **Standby**، او 10.1.1.1 Virtual IP ده.

HSRP Failover

که R1 ناکام شي:

R1 = Active ✗

↓

R2 = Standby

↓

R2 = Active

R2د Active رول اخلي او Hosts لا هم هماغه Virtual IP:

10.1.1.1

د Default Gateway په توګه کاروي.

IPv6 — Internet Protocol Version 6

IPv6 (Internet Protocol Version 6)د IP پروتوکول شپږمه نسخه ده چې د IPv4 د Address Space د محدوديت د حل لپاره رامنځته شوې ده. د کتاب له مخې، IPv6د **128-bit Address**کاروي، په داسې حال کې چې IPv4 د **32-bit Address**کاروي. د IPv6 Address Space له همدې امله ډېر لوی دی.

په CCNA 200-301 کې د IPv6 لپاره د **Addressing**او **Prefix Configuration/Verification** او د IPv6 Address ډولونه مهم دي.

د IPv6 Address بڼه

IPv6 Addressد **Hexadecimal**عددونو په وسيله ليکل کېږي او د :نښې په وسيله جلا کېږي.

مثال:

2001:DB8:ACAD:1::1/64

دلته:

2001:DB8:ACAD:1

د Network Prefix برخه ده، او:

::1

د Interface/Host برخه ښيي.

/64د IPv6 Prefix Length دی.

د IPv6 مهمAddress Types

د کتاب د CCNA Exam Topics له مخې لاندې IPv6 Address Types مهم دي:

1. Global Unicast

Global Unicast Addressد IPv6 هغه Address دی چې د Global Network Communication لپاره کارېږي.

مثال:

2001:DB8:ACAD:1::10/64

2. Unique Local

Unique Local Addressد داخلي Local/شبکو لپاره کارول کېږي او د Global Internet لپاره Routable نه وي.

3. Link-Local

Link-Local Addressد یوه Local Link دننه د ارتباط لپاره کارېږي.

د کتاب په Linux مثال کې Link-Local IPv6 Address داسې ښکاري:

fe80::e5b8:f355:636a:b2a4/64

او Scope يې linkښودل شوی.

4. Anycast

Anycast Addressد څو Interfaces سره تړل کېدای شي؛ Packet د ورته Address لرونکو Interfaces له ډلې مناسب/نږدې Interface ته رسېږي.

5. Multicast

Multicast Addressد څو Hosts یا Interfaces لپاره کارېږي.

6. Modified EUI-64

Modified EUI-64هغه میتود دی چې د Interface MAC Address پر بنسټ د IPv6 Interface ID جوړولو لپاره کارول کېږي.

دا ټول Address Types د CCNA 200-301 د IPv6 Addressing موضوع برخه دي.

IPv6 Prefix

IPv6د Network د برخې معلومولو لپاره **Prefix Length**کاروي.

مثال:

2001:DB8:ACAD:1::10/64

دلته:

/64

د Prefix Length دی.

په IPv4 کې د Subnet Mask مثال:

255.255.255.0

خو په IPv6 کې عموماً Prefix Length داسې ښودل کېږي:

/64

IPv6 Configuration Example

په Cisco Router کې د IPv6 Address Configuration لپاره:

```
R1(config)# ipv6 unicast-routing
R1(config)# interface GigabitEthernet0/0
R1(config-if)# ipv6 address 2001:DB8:ACAD:1::1/64
R1(config-if)# no shutdown
```

د Link-Local Address مشخص کولو مثال:

```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# ipv6 address FE80::1 link-local
```

د Interface Configuration داسې کېدای شي:

```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# ipv6 address 2001:DB8:ACAD:1::1/64
R1(config-if)# ipv6 address FE80::1 link-local
```

```
R1(config-if)# no shutdown
```

IPv6 Verification

د IPv6 Interface Address د کتلو لپاره:

```
R1# show ipv6 interface brief
```

د IPv6 Routing Table لپاره:

```
R1# show ipv6 route
```

د Interface بشپړ IPv6 معلوماتو لپاره:

```
R1# show ipv6 interface
```

IPv6د 128 bit Addressing-پروتوکول دی چې د IPv4 د 32 bit Addressing-په پرتله ډېر لوی Address Space لري. د CCNA لپاره د IPv6 په برخه کې **IPv6 Address، Prefix، Global Unicast، Unique Local، Link-Local، Anycast، Multicast**او **Modified EUI-64** مهم موضوعات دي.

Wide Area Network (WAN)

WAN (Wide Area Network)هغه Network دی چې د جغرافیایي پلوه په پراخه سیمه کې مختلف **LANs**او **Network Sites** سره نښلوي WAN .کولای شي د ښارونو، ولایتونو، هېوادونو او حتی د نړۍ په کچه شبکې سره وصل کړي.

مثال:

```
LAN ── Router ── WAN ── Router ── LAN
```

په ساده ډول:

```
Office A Office B
LAN LAN
| |
Switch Switch
| |
Router ======== WAN ============ Router
```

WANولې کارول کېږي؟

WANهغه وخت کارېږي چې مختلف Network Sites په یوه پراخه جغرافیایي سیمه کې موقعیت ولري او اړتیا وي چې له یو بل سره Network Communicationولري.

WANاو LAN توپیر

WAN	LAN	ګانګرتیا
Wide Area Network	Local Area Network	بشپړ نوم
پراخه	محدوده	ساحه
د مختلفو ښارونو دفترونه	د یوه دفترNetwork	مثال
RouterاوWAN Links	Switch/Router	اتصال
مختلف Sites نښلول	Local Devicesنښلول	هدف

WAN Connection

په WAN کې عموماً **Routers**د مختلفو Network Sites ترمنځ د ارتباط لپاره کارېږي.

```
PCs
↓
Switch
↓
Router
↓
WAN Link
↓
Router
```

↓
Switch
↓
PCs

Routerد مختلفو شبکو ترمنځPacket ونه Forward کوي.

WAN Configuration Example

د دوو Routers ترمنځ د WAN Link ساده مثال:

```
R1 R2
 | |
G0/1 G0/1
 | |
10.0.0.1 -------- 10.0.0.2
WAN Network
```

R1 Configuration

```
R1(config)# interface GigabitEthernet0/1
R1(config-if)# ip address 10.0.0.1 255.255.255.252
R1(config-if)# no shutdown
```

R2 Configuration

```
R2(config)# interface GigabitEthernet0/1
R2(config-if)# ip address 10.0.0.2 255.255.255.252
R2(config-if)# no shutdown
```

Connectivity Test

له R1 څخه:

```
R1# ping 10.0.0.2
```

له R2 څخه:

```
R2# ping 10.0.0.1
```

که Ping بریالی شي، د دواړو Routers ترمنځ IP Connectivity موجوده ده.

WANکې Routing

کله چې WAN له دوو څخه زیات Networks سره ونښلوي، Routerته د نورو Networks Routes هم پکار وي .په لاندې طریقو زده کېدای شي:

Static Routing

یا

Dynamic Routing

مثال:

```
LAN 1 — Router 1 ——— WAN ——— Router 2 — LAN 2
                    |
                Routing Table
```

Routerد Routing Table پر اساس ټاکي چې Packet باید کومې لارې ته واستول شي.

لنډه پایله

WANد پراخې جغرافیایي سیمې مختلف Networks یا Sites سره نښلوي **Router** .د WAN په جوړښت کې مهم رول لري، ځکه د مختلفو Networks ترمنځ Packetونه Forward کوي.

HDLC & PPP

د ورکړل شوي **CCNA 200-301 Volume 2**له مخې، **HDLCاو PPP** د WAN د Point-to-Point ارتباطاتو اړوند مهم Protocols دي. خو په دې ورکړل شوي Volume 2کې د **HDLCاو PPP بشپړ Configuration مثالونه** نه دي وړاندې شوي؛ نو زه به دلته یوازې هغه معلومات ولیکم چې سرچینه یې ملاتړ کوي، او Configuration به یوازې هغه وخت درکړم چې په کتاب کې موجود وي.

HDLC —— High-Level Data Link Control

HDLC (High-Level Data Link Control)د **Data Link Layer**یو Protocol دی چې د Point-to-Point WAN ارتباطاتو لپاره کارول کېږي.

د HDLC دنده دا ده چې د WAN Link پر سر د Data Frames انتقال تنظیم کړي.

Router R1
|
| HDLC |
|
Router R2

PPP —— Point-to-Point Protocol

PPP (Point-to-Point Protocol)د Point-to-Point WAN Links لپاره کارېدونکی Data Link Protocol دی.

PPPد HDLC په پرتله د Authentication او نورو امکاناتو لپاره پراخ ملاتړ لري.

Router R1
|
| PPP |
|
Router R2

PPP Authentication

PPPکې د Authentication لپاره مهم انتخابونه:

- **PAP —— Password Authentication Protocol**
- **CHAP —— Challenge Handshake Authentication Protocol**

د دې له لارې Router کولای شي د Point-to-Point Link په مقابل لوري کې خپل Peer Authenticate کړي.

PPPoE & MLPPP

PPPoE —— PPP over Ethernet

PPPoE (Point-to-Point Protocol over Ethernet)د PPP پروتوکول د Ethernet شبکې پر سر انتقالوي.

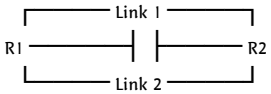
په ساده ډول:

Ethernet
↓
PPPoE
↓
PPP

PPPoEپه ځانګړي ډول هغه وخت مهم دی چې PPP Features د Ethernet-based Access Network له لارې استعمالېږي.

MLPPP —— Multilink PPP

MLPPP (Multilink Point-to-Point Protocol)د PPP هغه ځانګړتیا ده چې څو Physical Links د یوه Logical/Multilink ارتباط په توګه استعمالوي.



↓
MLPPP Bundle

یعنې د څو Links په یوځای کولو سره یو **Multilink Bundle**جوړېږي.

د ځلورو Protocols لنډ توپیر

اصلي مفهوم	بشپړ نوم	Protocol
Point-to-Point WAN Data Link	High-Level Data Link Control	**HDLC**
Point-to-Point WAN Protocol	Point-to-Point Protocol	**PPP**
PPPد Ethernet پر سر	PPP over Ethernet	**PPPoE**
څو PPP Links د یوه Logical Link په توګه Multilink PPP		**MLPPP**

مهمه یادونه

ستاسې د ورکړل شوي CCNA 200-301 Volume 2په موجوده محتوا کې د HDLC، PPP، IPPPoEاو MLPPP بشپړ Cisco Configuration Examples نه دي وړاندې شوي. له همدې امله زه دلته له کتاب څخه بهر Configuration Commands نه ورزیاتوم، ځو ستاسې د **«یوازې د ورکړل شوي کتاب له مخې»** اصول مراعات شي.

Circuit Switching — Packet Switching — MPLS — Metro Ethernet — Broadband

د ورکړل شوي CCNA 200-301 Official Cert Guide, Volume 2له مخې دا موضوعات د WAN Architectureله برخې سره تړاو لري. لاندې معلومات د همدې کتاب له محتوا څخه اخیستل شوي دي.

1. Circuit Switching

Circuit Switchingهغه طریقه ده چې د ارتباط لپاره مخکې له مخکې یو مشخص Dedicated Path/Circuitجوړېږي او د ارتباط په جریان کې هماغه Circuitکارول کېږي.

د WAN په پخوانیو ټیکنالوژیو کې د TDM/Serialلینکونو په ځېر ارتباطات د WAN د Access Links په توګه کارېدلي دي. کتاب د TDM لینکونو مثالونه T1, T3, E1, E3یادوي.

ساده تصور:

R1 ——————— Dedicated Circuit ——————— R2

د Circuit Switching مهم مفهوم دا دی چې د ارتباط لپاره ګانګړې لاره/سرکټ رامنځته کېږي.

2. Packet Switching

Packet Switchingکې Data په Packetsوېشل کېږي او Network د هر Packet د انتقال لپاره د Network معلومات کاروي.

د کتاب د IP Routing مثال:

R1 ⟶ R2 ⟶ R3 ⟶ R4

هر Router د Packet د Destination IP Address او خپل Routing Table پر اساس د Packet د راتلونکي انتقال پرېکړه کوي.

Packetله یوه Router څخه بل Router ته Forward کېږي.

Circuitاو Packet Switching توپیر

Packet Switching	Circuit Switching ګانګړتیا
Packets	Dedicated Circuit ارتباط
د Network د Routing پر اساس ګانګړېCircuit	لاره
IP Network	TDM/Serial WAN مثال
Packet-oriented	Circuit-oriented Forwarding

3. MPLS —— Multiprotocol Label Switching

MPLS (Multiprotocol Label Switching)د WAN Technology ده چې Service Provider پرې د مشتریانو ترمنځ IP-based WAN Serviceجوړوي. د MPLS Networkدننه د Packet Forwarding لپاره د Destination IP Address پر ځای MPLS Labelsکارول کېږي.

CE (Customer Edge):

د Customer په Site کې عموماً Router وي.

PE (Provider Edge):

د Service Provider د Network په Edge کې Router وي.

MPLS VPN

MPLS VPNاجازه ورکوي چې څو Customers د یوه MPLS Network څخه استفاده وکړي، خو د هر Customer Traffic او Routes له نورو Customers څخه جلا وساتل شي.

Customer A ┐

```
MPLS Network ──┤ جلا VPN
Customer B ──┘
```

MPLS VPNد Customer لپاره **Layer 3 Service** وړاندې کوي.

MPLS Configuration

مهم : د دې موضوع لپاره د کتاب په Customer-side برخه کې د MPLS بشپړ Cisco Configuration Example نه دی ورکړل شوی؛ کتاب د MPLS Architecture، CE/PE، VPN، Routingاو QoS مفاهیم تشریح کوي. نو له کتاب څخه بهر Configuration Command نه ورزیاتوم.

4. Metro Ethernet

Metro Ethernet (MetroE)د WAN Service یو ډول دی چې Customer ته د **Layer 2 Ethernet Service** ورکوي.

د MetroE په Network کې Customer Device د Service Provider Device سره د **Ethernet Access Link**له لارې وصلېږي Service Provider. د Customer Ethernet Framesله یوه Site څخه بل Site ته Forward کوي.

ساده جوړښت:

```
R1 ──── Ethernet ──┐
R2 ──── Ethernet ──┤
R3 ──── Ethernet ──┼── Metro Ethernet WAN
R4 ──── Ethernet ──┘
```

Metro Ethernetد Customer له نظره تقریباً داسې ښکاري لکه یوه لویه **Ethernet Switch**چې ټول Sites سره نښلوي.

Metro Ethernet Access Link

Customerاو Service Provider ترمنځ فزیکي لینک ته **Access Link** ویل کېږي، او د Ethernet په حالت کې ورته **Ethernet Access Link** ویل کېږي.

د دې ارتباط لپاره **UNI (User Network Interface)**اصطلاح هم کارېږي.

Metro Ethernet Service Types

Topology	لنډ نوم Service	
Point-to-Point	**E-Line**	Ethernet Line Service
Full Mesh	**E-LAN**	Ethernet LAN Service
Hub-and-Spoke / Partial Mesh / Point-to-Multipoint	**E-Tree**	Ethernet Tree Service

E-Line

```
R1 ──────────── MetroE ──────────── R2
```

یوازې دوه Customer Devices یو بل سره Ethernet Frames تبادله کوي.

E-LAN

```
   R1
  / \
 R2──R3
  \ /
   R4
```

ټول Devices کولای شي له یو بل سره مستقیم Ethernet Frames تبادله کړي.

E-Tree

```
   R1
  /\
 R2 R3
 | |
Leaf Leaf
```

Root Siteله Leaf Sites سره ارتباط لري، خو Leaf Sites له یو بل سره مستقیم ارتباط نه لري.

Metro Ethernet Configuration

د Metro Ethernet Service Provider داخلي Configuration د Customer له لوري نه کېږي. د کتاب په محتوا کې د **E-Line/E-LAN/E-Tree** لپاره د Customer-sideبشپړ Cisco Configuration نه دی ورکړل شوی؛ ځکه MetroE د Service Provider WAN Service دی.

5. Broadband

Broadbandد لوړ سرعت Internet Access ټکنالوژیو لپاره کارول کېږي. د کتاب د WAN Architecture له مخې مهم Broadband/Internet Access ټکنالوژۍ دا دي:

- **DSL**
- **Cable Internet**
- **4G/5G Wireless**
- **Fiber Ethernet**

DSL — Digital Subscriber Line

DSLد Telco موجوده **Telephone Copper Local Loop**کاروي او د لوړ سرعت Data انتقال لپاره کارول کېږي DSL .کولای شي د Telephone Voice او Digital Dataلپاره هماغه Telephone Line استعمال کړي.

PC
|
DSL Modem
|
Telephone Line
|
DSLAM
|
ISP Router
|
Internet

DSLAM (DSL Access Multiplexer)د Telco په Central Office کې د Voice او Data Signals جلا کوي؛ Data Router ته او Voice د Voice Switch/PSTNلوري ته استوي.

Cable Internet

Cable Internetد **CATV (Cable TV) Coaxial Cabling**څخه استفاده کوي.

PC
|
Cable Modem
|
CATV Cable
|
Cable Company
|
Router
|
Internet

د DSL په څېر Cable Internet هم عموماً **Asymmetric Speeds**لري، يعنې Downstream Speed د Upstream په پرتله لوړه وي.

4G/5G Wireless

Wireless WANد **Radio Waves**له لارې د Mobile Tower سره ارتباط جوړوي.

Laptop / Phone / Router
|
4G / 5G
|
Mobile Tower
|
Mobile Provider
|

Internet

د کتاب له مخې **3G، G4، LTEاو 5 G**د Wireless Internet Access مهم اصطلاحات دي Enterprise .هم کولای شي Router ته د 4 Card Wireless Gپه نصبولو سره دغه ډول Internet Access استعمال کړي.

Fiber Ethernet Internet

Fiber Internetد **Fiber-Optic Cabling**څخه استفاده کوي. د کتاب له مخې Fiber عموماً د Copper DSL او Cable په پرتله د اوږدو واټنونو لپاره لوړ سرعت وړاندې کوي. ځینې ISP ګانې Fiber Internet د **Ethernet Protocols over Fiber**په وسیله وړاندې کوي.

Router

|

Fiber

|

ISP

|

Internet

Broadbandلنډه پرتله

مهم**Device**	**Medium**	**Technology**
DSL Modem / DSLAM	Telephone Copper	**DSL**
Cable Modem	CATV Cable	**Cable Internet**
Mobile Tower / Wireless Router	Radio/Wireless	**4G/5G**
Fiber/Ethernet Equipment	Fiber Optic	**Fiber Ethernet**

مهمه یادونه

د **Circuit Switching، MPLS، Metro Ethernetاو Broadband** په دې موضوعاتو کې کتاب زیاتره **WAN Architectureاو Concepts** تشریح کوي. د MPLSاو Metro Ethernet لپاره د Customer له اړخه بشپړ Cisco CLI Configuration نه دی ورکړل شوی؛ نو د کتاب د اصولو مطابق مې له ځانه Configuration Commandsنه دي اضافه کړي.

VPN — Virtual Private Network

VPN (Virtual Private Network)هغه امنیتي ټکنالوژي ده چې دوه Devices د یوه ناامنNetwork ، لکه **Internet**، له لارې په داسې ډول سره نښلوي چې Data په خوندي ډول انتقال شي .د VPN Private WAN په څېر د خوندي ارتباط ځانګړتیاوې برابروي، خو د عام Internet پر سر کار کوي.

د VPN مهمې امنیتي دندې

VPNد لاندې امنیتي ځانګړتیاوو لپاره کارېږي:

- — **Confidentiality (Privacy)**د Data محرمیت ساتي او د منځګړي کس لپاره Data د لوستلو وړ نه وي.
- — **Authentication**معلوموي چې د VPN Packet لېږونکی مجاز Device دی.
- — **Data Integrity**معلوموي چې Data د انتقال پر مهال بدله شوې که نه.
- — **Anti-Replay**د یوه معتبر Packet د بیا استعمال مخه نیسي.

VPN Tunnel

VPNعموماً د دوو Edge Devices ترمنځ یو **VPN Tunnel**جوړوي.

Office A Office B

LAN LAN

| |

R1 ============================== FW1

Secure VPN Tunnel

|

Internet

د VPN Devices اصلي IP Packet ته اضافي Headers ورزیاتوي او Original IP Packet Encrypt کوي. له همدې امله که څوک Packet د Internet په منځ کې ترلاسه کړي، د Original Data محتوا نه شي لوستلای.

Site-to-Site VPN

Site-to-Site VPNد دوو Sites ترمنځ د VPN ارتباط لپاره کارېږي.

مثال:

```
Office A Office B
| |
Router A ===== Internet ===== Router B
VPN Tunnel
```

په دې ډول VPN کې د هر Site ټول Devices د یوه VPN Tunnel له لارې ارتباط کولای شي. هر PC ته جلا VPN جوړولو اړتیا نشته.

IPsec Site-to-Site VPN

IPsecد IP Networks لپاره د Security Services یو Architecture/Framework دی IPsec .د VPN لپاره د **Confidentiality، Authentication، Data Integrity**او **Anti-Replay** ځانګړتیاوې برابروي.

د کتاب په مثال کې **GRE Tunnel + IPsec**یوځای کارول کېږي:

```
R1 ========================== R2
GRE Tunnel + IPsec
|
Internet
```

GREد Tunnel مفهوم رامنځته کوي، او IPsec د Tunnel له لارې د تېرېدونکي Data لپاره Security برابروي.

Remote Access VPN

Remote Access VPNهغه وخت کارېږي چې یوIndividual Device ، لکه **PC**، د خپل VPN Connection له لارې Enterprise Network ته وصل شي.

```
Laptop
|
Internet
|
VPN Firewall
|
Enterprise Network
```

د Site-to-Site VPN برعکس، Remote Access VPNکې یو User Device خپله VPN Connection جوړوي.

TLS Remote Access VPN

Remote Access VPNsډېر وخت له **TLS (Transport Layer Security)**څخه استفاده کوي.

د کتاب له مخې، **Cisco AnyConnect Secure Mobility Client**په PC کې نصب کېدای شي او د TLS په وسیله VPN Tunnel جوړوي؛ د Tunnel له لارې د PC ټول Traffic Encrypt کېدای شي.

Remote Access VPNاوSite-to-Site

ځانګړتیا	Site-to-Site VPN	Remote Access VPN
Typical Security Protocol	**IPsec**	**TLS**
Devices	ډېرDevices	یوDevice
Connection	عموماًPermanent	عموماًOn-Demand
مثال	Office ↔ Office	Laptop ↔ Enterprise

VPN Configuration Example

مهم:ستاسې د ورکړل شوي **CCNA 200-301 Volume 2**په دې VPN برخه کې د بشپړ **IPsec/GRE VPN CLI Configuration** Cisco مثال نه دی ورکړل شوی. کتاب دVPN Architecture ، IPsec، GRE، Site-to-Siteاو Remote Access مفاهیم تشریح کوي، نو زه له کتاب څخه بهر Configuration Commandsنه ورزیاتوم.

د VPN د عملي جوړښت مثال

Site A Site B

192.168.1.0/24 192.168.2.0/24

| |

R1 ============================ R2

IPsec VPN Tunnel

|

Internet

په دې Architecture کې R1 او R2 د VPN Tunnel Endpoints دي او د دواړو Sites ترمنځ Traffic د VPN له لارې په خوندي ډول انتقالېږي.

لنډه پایله

VPN

↓

Secure Tunnel

↓

Encryption + Authentication

↓

Data Integrity + Anti-Replay

↓

Secure Communication over Internet

VPNد عام Internet پر سر د Private او Secure Network Communication لپاره کارېږي، او په CCNA کې يې مهم ډولونه **Site-to-Site VPN**او **Remote Access VPN**دي.

GRE — BGP — AAA

1. GRE — Generic Routing Encapsulation

GRE (Generic Routing Encapsulation)يو **Tunneling Protocol**دی چې د مختلفو Network Protocols يا Packets د انتقال لپاره يو منطقي Tunnel جوړوي.

د کتاب له مخې، GREد VPN په جوړښت کې د Tunnel د جوړولو لپاره کارېدلی شي، خو GRE پخپله د Data د Encryption لپاره Security نه برابروي. له همدې امله **GRE + IPsec**يوځای کارول کېدای شي؛ GRE Tunnel جوړوي او IPsec د Traffic امنيت برابروي.

GREساده جوړښت

Site A Site B

R1 ============================ R2

GRE Tunnel

|

Internet

GRE Configuration Example

د کتاب په ورکړل شوي Volume 2 کې د GRE بشپړ Cisco CLI Configuration Example نه دی وړاندې شوی. نو د کتاب د اصولو مطابق دلته له ځانه Configuration Commandsنه اضافه کوم.

2. BGP — Border Gateway Protocol

BGP (Border Gateway Protocol)د Dynamic Routing Protocols له ډلې څخه دی او د مختلفو **Autonomous Systems (AS)**ترمنځ د Routing Informationد تبادلې لپاره کارېږي.

د کتاب له مخې، BGPد Routerد **Control Plane**له Routing Protocols څخه دی، لکه:

OSPF

EIGRP

RIP

BGP

دا Routing Protocols د Routing Table د جوړولو، بدلولو او تازه کولو لپاره کار کوي.

BGPساده جوړښت

AS 100

|

R1

|

eBGP

|

R2

|

AS 200

دلته R1 او R2 د مختلفو Autonomous Systems برخه دي او BGP د دوی ترمنځ د Routing Information د تبادلې لپاره کارول کېدای شي.

BGP Configuration Example

د ورکړل شوي **CCNA 200-301 Volume 2**په موجوده محتوا کې د BGP بشپړ Cisco Configuration Example نه دی وړاندې شوی؛ نو له کتاب څخه بهر router bgp Configurationنه اضافه کوم.

3. AAA —— Authentication, Authorization, and Accounting

AAAد Network Security یو Framework دی چې د User Access د کنټرول لپاره درې مهمې دندې لري:

Authentication

Authenticationمعلوموي چې User واقعاً څوک دی.

Who are you?

مثال:

Username + Password

Authorization

Authorizationمعلوموي چې Authenticated User کومو Resources یا Commands ته اجازه لري.

What are you allowed to do?

مثال:

User ⟶ Accessمحدود

Admin ⟶ Privileged Access

Accounting

Accountingد User د فعالیتونو او Access په اړه معلومات ثبتوي.

What did you do?

لکه:

Login

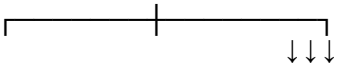
Logout

Access Activity

AAAدرې برخې

AAA

|



Authentication Authorization Accounting

Who are What can What did

you? you do? you do?

AAA Configuration Example

د کتاب په موجود **Volume 2**کې د AAA د بشپړ Cisco IOS Configuration مثال نه دی وړاندې شوی. له همدې امله، د کتاب د سرچینې د اصولو مطابق، دلته له ځانه Configuration Commands نه ورزیاتوم.

لنډه پايله

اصلي دنده	موضوع
Tunnelجوړول	**GRE**
د Routing Information تبادله، په ځانګړي ډول د Autonomous Systems ترمنځ	**BGP**
Authentication، Authorizationاو Accounting	**AAA**

يادونه : د دې درې واړو لپاره مې يوازې هغه معلومات وړاندې کړل چې ورکړل شوي **CCNA 200-301 Volume 2**يې ملاتړ کوي؛ دGRE ، IBGPاو AAA بشپړ CLI Configuration چې په کتاب کې نشته، قصداً مې نه دی ورزيات کړی.

1. NTP & Syslog

1.1 NTP —— Network Time Protocol

NTPڅه شی دی؟

NTP (Network Time Protocol)هغه Network Protocol دی چې د کمپيوټرونو، Routerونو، Switchونو، Serverونو او نورو Network Devices ترمنځ د وخت د برابرولو لپاره کارېږي.

په يوه Network کې کېدای شي لسګونه يا سلګونه وسايل موجود وي. که د هر Device ساعت مختلف وي، نو د Network د Events او Logs د تحليل پر مهال ستونزه پيدا کېږي.

د مثال په توګه:

Router 10:30:15

Switch 10:35:42

Server 10:28:07

که په Router کې يوه ستونزه په 10:30رامنځته شوې وي، خو Server کې وخت 10:28وي، نو Administrator ته به معلومول ستونزمن وي چې Event په ريښتيا څه وخت رامنځته شوی.

NTPدا ستونزه حل کوي او د Network Devices وخت د يوه معتبر Time Source سره Synchronize کوي.

1.2 NTP څنګه کار کوي؟

NTPعموماً د يوه **NTP Server**څخه د دقيق وخت معلومات اخلي.

مثلاً:

NTP Server

192.168.1.10

|

| | |

Router Switch Server

Router، Switchاو Server د NTP Server څخه وخت اخلي او خپل ساعت ورسره Synchronize کوي.

NTPد **UDP Port 123**کاروي.

1.3 NTPولې مهم دی؟

NTPپه لاندې مواردو کې ډېر مهم دی:

- د Network Devices د وخت برابرول
- د Syslog Messages دقيق Timestamp
- د Network Troubleshooting
- د Security Events تحليل
- د Authentication او Logging لپاره دقيق وخت
- د مختلفو Servers او Devices ترمنځ Time Synchronization

1.4 Cisco Routerکې دNTP Configuration

فرض کړئ زموږ NTP Server دا IP Address لري:

192.168.1.10

په Router کې:

```
Router(config)# ntp server 192.168.1.10
```

د NTP حالت معلومولو لپاره:

```
Router# show ntp status
```

د NTP Server سره د Association معلومولو لپاره:

```
Router# show ntp associations
```

د Router اوسنی وخت معلومولو لپاره:

```
Router# show clock
```

2. Syslog

2.1 Syslog څه شی دی؟

Syslogیو سیستم/پروتوکول دی چې Network Devices خپل مهم Events او Messages مرکزي ځای ته د ثبت او Monitoring لپاره استوي.

مثلاً په Router کې Interface Down شي:

```
Interface GigabitEthernet0/0 is down
```

یا یو Administrator Configuration بدله کړي.

دغه Events د Syslog Server له لارې ثبت او وروسته کتلی شو.

2.2 Syslog ولې مهم دی؟

فرض کړئ په یوه شرکت کې Router50 ونه اوSwitch ونه موجود دي.

که هر Device خپل Logs یوازې په خپل داخلي حافظه کې وساتي، Administratorباید هر Device جلا وګوري.

Syslogدا کار اسانه کوي:

```
Router 1 ----\
Router 2 -----\
Switch 1 ------> Syslog Server
Switch 2 -----/
Router 3 ----/
```

ټول مهم Logs یوه مرکزي Server ته استول کېږي.

2.3 Syslog کوم معلومات ثبتوي؟

Syslogکولی شي د لاندې Events معلومات ثبت کړي:

- Interface Up/Down
- Hardware Errors
- Configuration Changes
- Authentication Events
- System Warnings
- Network Errors
- Routing Events
- Security-related Events

2.4 Syslog Port

Syslogعموماً:

```
UDP 514
```

کاروي.

2.5 Syslog Severity Levels

Syslog Messagesد اهمیت له مخې له **0تر 7** پورې طبقه‌بندي کېږي.

Level	نوم	تشریح
0	Emergencies	سیستم تقریباً unusable دی
1	Alerts	سمدستي اقدام ته اړتیا لري
2	Critical	جدي ستونزه
3	Errors	Errorرامنځته شوی
4	Warnings	خبرداری
5	Notifications	مهم عاديEvent
6	Informational	معلوماتي پیغام
7	Debugging	د Debugging معلومات

مهم اصل

0تر ټولو لوړ Severity لري او 7 تر ټولو ټیټ.

یعني:

= 0ډېر جدي

= 1جدي

2 = Critical

3 = Error

4 = Warning

5 = Notification

6 = Information

7 = Debug

2.6 Ciscoکې Syslog Configuration

فرض کړئ:Syslog Server

192.168.1.20

Routerکې:

```
Router(config)# logging host 192.168.1.20
```

د Logging معلوماتو د کتلو لپاره:

```
Router# show logging
```

3. SNMP — Simple Network Management Protocol

3.1 SNMP څه شی دی؟

SNMP (Simple Network Management Protocol)د Network Devices د **Monitoring**او **Management** لپاره کارېږي.

د SNMP له لارې Network Administrator کولی شي معلوم کړي چې:

- Routerڅومره Traffic لري؟
- Interfaceڅومره Packets لېږدوي؟
- Interface Upدی کهDown ؟
- CPUڅومره استعمالېږي؟
- Memoryڅومره استعمالېږي؟
- Deviceڅومره وخت کېږي چې Restart شوی؟
- کوم Interface Error لري؟

3.2 SNMP څنګه کار کوي؟

SNMPعموماً د درې مهمو برخو له لارې کار کوي:

1. SNMP Manager

SNMP Managerهغه Management System دی چې Network Devices Monitor کوي.

2. SNMP Agent

SNMP Agentپه Network Device کې موجود Software/Service دی چې د Device معلومات راټولوي او SNMP Manager ته يې ورکوي.

3. MIB

MIB (Management Information Base)هغه جوړښت دی چې د Device د Management معلوماتو تعريف پکې موجود وي.

عملي جريان:

SNMP Manager

|

SNMP Request

|

v

Router/Switch

SNMP Agent

|

v

MIB

3.3 SNMP Ports

SNMPعموماً لاندې UDP Ports کاروي:

UDP 161 ⟶ SNMP Queries

UDP 162 ⟶ SNMP Traps

SNMP Query

Managerله Device څخه معلومات غواړي.

مثلاً:

CPU Usageڅو سلنه دی؟

SNMP Trap

Devicپخپله Manager ته مهم Event استوي.

مثلاً:

Interface GigabitEthernet0/0 is DOWN

3.4 SNMP Versions

SNMPv1

د SNMP لومړنی نسخه ده او Security يې محدوده ده.

SNMPv2c

د v1 په پرتله ښه امکانات لري، خو د Security لپاره يې Community String کارېږي.

SNMPv3

د Security له نظره تر ټولو پرمختللې نسخه ده او د Authentication او Encryption امکانات لري.

3.5 Cisco SNMP Configuration

مثلاً د Read-Only Community String جوړول:

```
Router(config)# snmp-server community CiscoRO RO
```

دلته:

CiscoRO = Community String

RO = Read Only

د SNMP Manager/Server مشخص کول:

```
Router(config)# snmp-server host 192.168.1.50 version 2c CiscoRO
```

4. IP SLA — IP Service Level Agreement

4.1 IP SLAڅه شی دی؟

IP SLA (IP Service Level Agreement)د Cisco یوه ځانګړنه ده چې د Network د Service او Connectivity Performance اندازه کولو لپاره کارېږي.

په ساده ډول:

IP SLA Routerته اجازه ورکوي چې Network په اتومات ډول Test او Monitor کړي.

Administratorکولی شي معلوم کړي چې یو Remote Device یا Network Service:

- Reachableدی که نه؟
- Response Timeيې څومره دی؟
- Delayڅومره دی؟
- Packet Lossشته که نه؟
- Network Serviceفعال دی که نه؟

4.2د IP SLA عملي مثال

فرض کړئ شرکت دوه Internet Connections لري:

```
Internet
/ \
ISP-1 ISP-2
| |
----------
|
Router
```

موږ غواړو Router په دوامداره توګه ISP-1 Test کړي.

که ISP-1 کار ونه کړي، Routerکولی شي د Routing Configuration له مخې بل Link استعمال کړي.

IP SLAدلته د Network Health معلومولو لپاره کارېږي.

4.3 IP SLA Configuration

فرض کړئ موږ غواړو دا IP Address Test کړو:

```
192.168.1.1
```

لومړی IP SLA جوړوو:

```
Router(config)# ip sla 1
```

د ICMP Echo Test ټاکو:

```
Router(config-ip-sla)# icmp-echo 192.168.1.1
```

Testهر 10 ثانيې وروسته ترسره کوو:

```
Router(config-ip-sla)# frequency 10
```

له Configuration Mode څخه وځو:

```
Router(config-ip-sla)# exit
```

IP SLAفعالوو:

```
Router(config)# ip sla schedule 1 life forever start-time now
```

4.4د IP SLA معلومات معلومول

د:IP SLA Statistics

```
Router# show ip sla statistics
```

د:IP SLA Configuration

```
Router# show ip sla configuration
```

5. Cisco Three-Layer Hierarchical Model

5.1 Hierarchical Modelڅه شی دی؟

Cisco Three-Layer Hierarchical Modelد Enterprise Network د ډیزاین لپاره یو منظم Architecture دی.

په دې Model کې Network په درېیو اصلي Layers وېشل کېږي:

1. **Access Layer**

2. **Distribution Layer**
3. **Core Layer**

اصلي هدف دا دی چې:Network

- منظم
- Scalable
- Reliable
- Manageable
- High Performance

وي.

5.2 Access Layer

Access Layerد Network هغه برخه ده چې End Devices ورسره مستقیم Connect کېږي.

لکه:

- Computer
- Printer
- IP Phone
- Access Point
- Camera

مثال:

PC
|
|
Access Switch
|
Access Layer

د Access Layer مهم کارونه

- End Devices Connectکول
- VLAN Accessبرابرول
- Port Security
- Access Control
- Basic Network Connectivity

مثلاً:

PC 1 ----\
PC 2 ----- Access Switch
Printer --/

دا ټول Devices د Access Layer له لارې Network ته داخلېږي.

5.3 Distribution Layer

Distribution Layerد Access Layer او Core Layer ترمنځ موقعیت لري.

دا Layer د Network Traffic د Control او Routing لپاره ډېر مهم دی.

د Distribution Layer مهم کارونه

- Inter-VLAN Routing
- Routing Policies
- ACL
- Traffic Filtering
- Route Summarization

- Redundancy
- د Access Layer Traffic کنټرول

Inter-VLAN Routing

فرض کړئ موږ دوه VLANs لرو:

VLAN 10 ⟶ Administration

VLAN 20 ⟶ IT

که د VLAN 10 او VLAN 20 ترمنځ Communication ته اړتیا وي، Distribution Layerکولی شي Routing ترسره کړي.

5.4 Core Layer

Core Layerد Network Backbone دی.

دا Layer د Network مختلفې برخې په ډېر لوړ سرعت سره له یو بل سره نښلوي.

مثال:

Core

/ \

/ \

Distribution Distribution

/ \ / \

Access Access Access Access

د Core Layer مهم هدف

Core Layerباید:

- Fast
- Reliable
- Highly Available
- Low Latency

وي.

Core Layerد User-level Policy او پیچلو Filtering کارونو لپاره نه، بلکې د **High-Speed Transport**لپاره ډیزاین کېږي.

5.5د درېیو Layers اړیکه

د یوه لوی شرکت مثال واخلو:

Internet

|

Router

|

CORE LAYER

/ \

/ \

DISTRIBUTION DISTRIBUTION

/ \ / \

/ \ / \

ACCESS ACCESS ACCESS ACCESS

| | | |

PCs Phones PCs APs

د دې Architecture په یاد ساتلو لپاره:

Access = Connect

Distribution = Control & Route

Core = Fast Transport

د ټول درس مهمه خلاصه

مهمPort/Protocol	اصلي دنده	موضوع
UDP 123	د Devices وخت Synchronize کول	**NTP**
UDP 514	د Events او Logs مرکزي ثبت	**Syslog**
UDP 161/162	Network Devices Monitoringد	**SNMP**
	د Operation مطابق د Network Performance او Connectivity اندازه کول	**IP SLA**
—	End Devices Connectکول	**Access Layer**
—	Routingاو Policy	**Distribution Layer**
—	High-Speed Backbone	**Core Layer**

د یادولو لپاره ساده فورمول

NTP ⟶ Time

Syslog ⟶ Logs

SNMP ⟶ Monitoring

IP SLA ⟶ Testing/Performance

Access ⟶ Connect

Distribution ⟶ Control/Route

Core ⟶ Transport

دا ترتیب د CCNA د زده‌کړې لپاره مناسب دی، ځکه هره موضوع لومړی **مفهوم**، بیا **د کار کولو طریقه**، وروسته **اصلي Components/Ports** او په پای کې **Cisco Configurationاو عملي مثال** تشریح کوي.