CCNA Summary Notes

Spanning Tree Protocol (802.1D)

NB. These notes were created around 2009.

Newer versions of CCNA R&S have been released since then, however these notes will still cover a large portion of the material.

Problems with redundant links
- Broadcast Storms
- Duplicate frame transmission
- MAC database instability (Host A is on port 1, no wait… port 2)

Layer 2 can't deal with these (layer 3 can with TTL etc but layer 2 can't)
Switches send broadcast packets out all of its interface except the one upon which it was received.

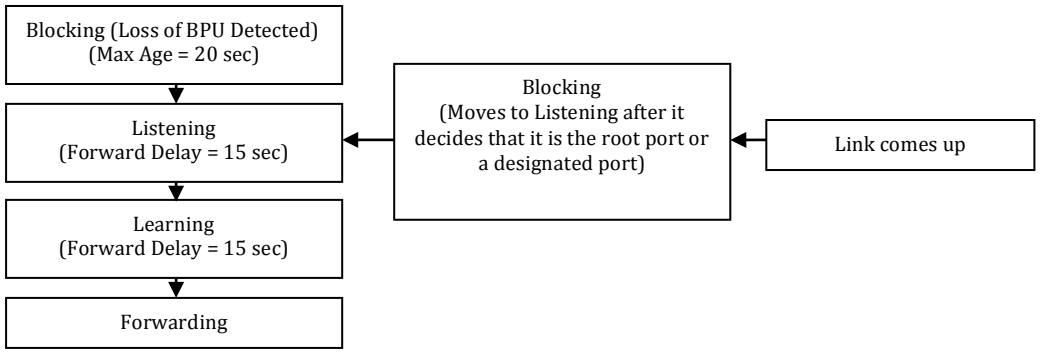
STPs 3 steps
STP puts some ports into a standby state where they do not listen to, forward, or flood data frames. Only one path to any given network segment at one time.

1. Elect a root bridge – all ports are designed
2. Selects the root port on the non-root bridges (bridge = switch). Root port is closest to root bridge based on accumulated bandwidth.
3. Select the designated port on each segments. This is based on lowest cost to root bridge (or BID if cost is equal).

BPDUs are exchanged every 2 seconds. Lowest BID = root.

The Bridge ID (BID) is included in BPDUs. BID = 2 btye bridge priority (32768 default) + 6 byte MAC.

When STP is enable all ports transition through blocking → Listening → Learning and then stabilize on forwarding or blocking.



When a switch boots up it assumes that it is the root bridge and moves from the Bocking to the Listening state. If it is in the Blocking state for the Max Age and receives no BPDUs it moves to the Listening states. Whilst in the Listening state it sends and receives the BPDUs to determine the topology. It does not pass any user data. It does the 3 STP steps in this state. Spends 15 seconds in this state. THE LEARNING SATE REDUCES THE AMOUNT OF FLOODING REQUIRED WHEN DATA BEGINS FORWARDING. After 15 seconds it moves to the forwarding (root or designated) or blocking (non designated) state. In the blocking state the port with receive BPDUs but not send data.

PortFast

PortFast is used to send port straight to forwarding state (e.g. if it is attached to PC). Does not have to wait for STP convergence. It has BPDU port guard which will disable the port if a BPDU is received to prevent routing loops.
Switch(config-if)#spanning-tree portfast
Switch(config-if)#spanning-tree portfast bpdu-guard (use no command to disable)
Switch(config)#spanning-tree portfast default (enable portfast on all acces ports)
Switch#show run int *interface* (shows if portfast has been enabled)

Path Costs

10 Gbps	2	
1 Gbps	4	Normal time to convergence for STP is 30-50seconds.
100 Mbps	19	
10 Mbps	100	

Other types of spanning Tree

PVST+ (Per VLAN Spanning Tree)
Uses more CPU and bandwidth.
BID has an extra VID (VLAN ID) field by taking up part of the Priority field. 12 bits of the 2 byte priority field are now for an extended system ID.

Rapid Spanning Tree Protocol
802.1w → faster convergence. Now has a backup state option for ports.
Port Roles are as follows:
Root→ forwarding port (same as STP)
Designated → forwarding port elected for every switch LAN segment (same as STP)
Alternate→ Alternate path to the root bridge.

Backup → Provides a redundant, less desirable, connection to another switch. Only exist where two ports are connected on a loopback by point-to-point OR where a bridge has two connections to the same shared VLAN segment.
Disabled → Plays no role.
Learning and forwarding are identical in RSTP and STP. Everything else is RSTP is discarding.

Switch(config)#spanning-tree mode rapid-pvst (enables PVRST+)
Switch#show spanning-tree vlan *vlan_number* [detail] (shows info per VLAN)
Switch#debug spanning-tree pvst+ (debugs PVRST+ evetns)
Switch#debug spanning-tree switch state (debugs port state changes)

PVRST+ (Per VLAN Rapid Spanning Tree)
Combines the above 2 methods.

Multiple Spanning Tree Protocol
Can have multiple VLANs all with one spanning tree instance. Mergews 802.1Q-2003.

Selecting the root bridge – make it centralised.
Switch#spanning-tree vlan *vlan_number* root [primary|secondary] … to set root bridge or backup (you can have multiple backups)

Security

Things to consider when inserting new equipment

1. Consider current Security Policies
2. Secure switch access

A well established policy has these features:

- You can audit the security setup
- Framework
- Defines how to treat unwanted electronic data
- Procedures
- Consensus amoung decision makes
- Incident management

- Enterprise wide plan

Securing switching devices

- Enable secret password
- G00d passwords
- Console and vty security (passwords and ACLs)
- Use SSH not telnet (cisco used v1. No plaintext is sent)
- Disable integrate HTTP daemon if not used. If needed use ACLs.
- Warning banners
- Disable unneeded services. no serice [tcp-small-servers|finger|config]
- Configure basic logging
- Encrypt password (service pw-en)

Securing switch protocols

- Managed CDP. So reconnaissance cannot attacks can't take place. Disable globally if not needed. Disable per port if needed.
- Secure STP. See root and backup bridges manually. Use BPDU guard.

Mitigating compromises launched through a switch

- Disable unused ports or put them in a "parking-lot" vlan as access ports.
- Disable automatic negotiation of Trunking (DoS, rediection etc are threats). PW VTP.
- Monitor PHYSICAL placement.
- Port based security. **swithport host** puts port in access with no channelling and STP portfast. ***no*** will reverse it . ***default interface*** returns interface back to default

Using "port security" feature

This is used on a switch to accept only particular MAC addresses.

- Dynamic – you care about how many rather than the specific MAC addresses that connect.
- Static – specify MAC addresses that are allowed.
- Combination of static and dynamic.

- Sticky Learning – dynamically learn a MAC and then add it to a static table.

If unauthorised MAC attempts to connect switch can shutdown port. Or add MAC to disallowed list and log.

802.1X Port-based authentication

Client requests access to switch. Switch communicates with authentication server. Until authentication takes place only Extensible Authentication Protocol over LAN (EAPOL) traffic is allowed through the switchport.

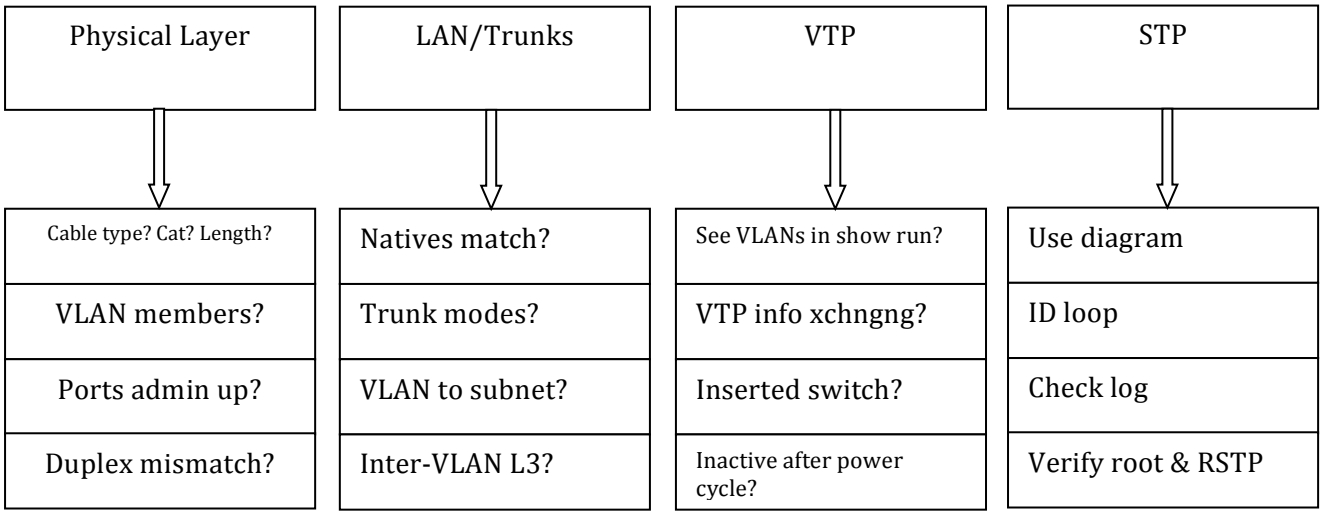
Client – needs 802.1X software client (XP offers this). Port that the client is attached to is called the client/supplicant.

Authentication server – Gives the permit/deny to the proxy switch. Is invisible to the client. RADIUS with EAP is the only supported server.

Switch – Controls the physical access based on the authentication status.Proxy. Has a RADIUS software client. En/decapsulates EAP frames.

Port is initially in authorised state. Goes to authorised once server says so. If switch asks for clients ID (authentication initiator)and client doesn't support 802.1X … tough. If client sends an EAPOL-start frame and gets no response (no 802.1X on switch) it just sends away. When a client logs out → send EAPOL-log message → change back to unauthorised.

Troubleshooting switches



EIGRP (the hybrid)

Rapid covergence using DUAL. Sends periodic update about only the parts that are needed. PDMs are used. Uses multicast and unicast. NO BROADCAST. Easy summarisation anywhere in the network.

EIGRP has a NEIGHBOUR TABLE and a TOPOLOGY TABLE.

Successor route → Best route to destination

Feasible successor → backup route

Advertised distance → Distance for a NEIGHBOUR to reach a network

Feasible disable → Distance to the neighbour + advertised distance

For a route to become a feasible successor (backup), a next-hop router must have an Advertised distance that is less that the feasible distance of the current router (i.e. the neighbour must be close to the destination than the current router).

Summarisation

EIGRP will automatically summarise at a classful boundary. You may not want this if you have discontiguous networks. Use the **no auto summary** command to disable auto-summarisation.

Load balancing across unequal paths

2 conditions must be met:
-Next router in path must be closer
- current feasible distance * variance (* = 'multiplied by'). If the alternative route does not fit under this you can't use it.

Metric

Bandwidth and delay

Configure

RouterA(config)#router eigrp 100 (100 is the AD number – no need to register)
RouterA(config-router)#network 192.168.3.0
RouterA(config-router)#network 192.168.4.0
RouterA(config-router)#no auto-summary
RouterA(config-router)#variance 5 (Metric of the alternative path as to be within
RouterA(config-router)#exit
RouterA(config)#interface fa0/1
RouterA(config-if)#bandwidth *bandwidth-in-kbps*

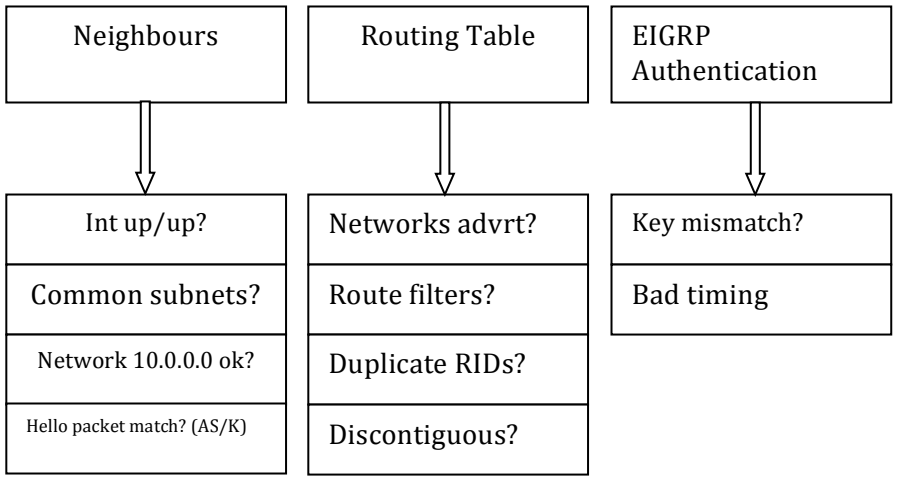
Show commands

Show ip protocols	(show metrics and parameters of current protocols)
show ip eigrp neighbors	(show neighbours)
show ip eigrp neighbors	(shows ints with EIGRP – can specify int or AS)
show ip route eigrp	(routing table EIGRP details)
show ip eigrp topology	(shows all learned routes)
debug eigrp neighbors	(show neighbour states and hello packets)
debug eigrp packets	(view neighbour adjacency process)

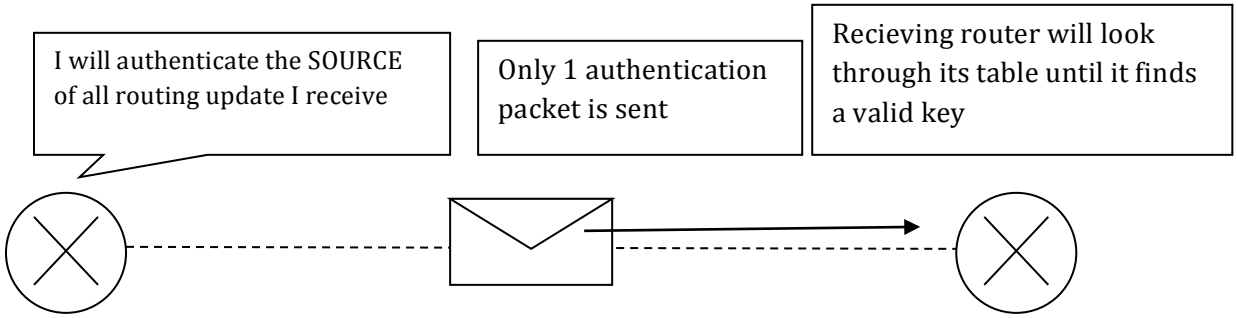
Authentication

RouterA(config)#interface fa0/1
RouterA(config-if)#ip authentication mode eigrp *process-id* **md5**
RouterA(config-if)#ip authentication key-chain eigrp *process-id key-chain*
RouterA(config-if)#exit
RouterA(config)#key chain *name-of-key-chain* *(create the chain)*
RouterA(config-chain)#key *number* *(create a key)*
RouterA(config-chain-key)#key-string *text* *(text is the password)*
RouterA(config-chain-key)#accept-lifetime 04:00:00 Jan 1 2006 04:01:00 Jan 1 2006
RouterA(config-chain-key)#send-lifetime 04:00:00 Jan 1 2006 infinite

Troubleshooting



EIGRP Key



Key ID (password) + interface = Authentication Key

RouterA(config)#interface fa0/1
RouterA(config-if)#ip authentication mode eigrp *process-id* **md5**
RouterA(config-if)#ip authentication key-chain eigrp *process-id key-chain*
RouterA(config-if)#exit
RouterA(config)#key chain *name-of-key-chain*
RouterA(config-chain)#key *number*
RouterA(config-chain-key)#key-string *text*

KEY CHAIN 1

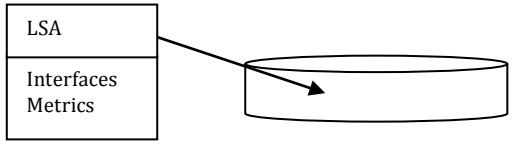
KEYS	DEFINITIONS
Authentication Key	Active from 9am – 10am
Authentication Key	Active from 9.55am – 11am
Authentication Key	Active from 10.55am – 12am
Authentication Key	Active from 11.55am – 1pm

OSPF

Link (interface information) state. Collection of Link states forms a link state database.

LSA

Sent every 30 minutes or when something changes.



Topological database

An overall view of the network. All routers in same area have identical topological DB

Hierarchy

Autonomous System (Domain) → Area

Each AS must have a backbone. Off that backbone can hang STUB AREAS, TOTALLY STUB AREAS, NSSA to help routing table size.

Area Border Routers connect multiple areas to the backbone router. ABR advertises a default router to the backbone router. ASBR is the border for an AS.

Neighbour adjacencies

Established using the HELLO protocol. Bidirectional communication = router sees itself in hello packet of neighbour.
224.0.0.5 is multicast address that HELLO packets are sent out on.

HELLO PACKET
Router ID – 32 bit loopback address acting as ID (no loopback=highest IP)
Hello interval – How often packets are sent. Default = 10s (30 sec s on non-broadcast link).
Dead interval – How long router will wait before declaring neighbour out of service (4 times hello)
Neighbours – Adjacent routers with bi-directional communication.
Area ID – Needs to be the same.
Router priority – 8 bit number used to determine who is DR and BDR.
IP of DR And BDR
Authentication – if enabled must swap same PW.
Stub Area Flag – Helps to reduce routing table size by providing default route.

SPF Algorithm

Dijkstra's algorithm puts router at root and calculates best path to all other nodes. LSAs are flooded.

Metric

Metric = 100,000,000 / speed in bps (higher bandwidth = lower & better cost)

To change the reference bandwidth use **ospf auto-cost reference-bandwidth** *ref-bw* command.

Configure

RouterA(config)#clear ip ospf process	(restarts all OSPF processes)
RouterA(config)#router ospf 100	(100 is the process id. Need not match)
RouterA(config-router)#network 192.168.3.0 0.0.0.255 area 0	(8 bit boundaries is bad)
RouterA(config-router)#network 192.168.4.0 0.0.0.255 area 0	
RouterA(config-router)#maximum-paths 6	(default 4. Up to 16)
RouterA(config-router)#exit	
RouterA(config)#interface lo0/1	(loopback interface is used as ID)
RouterA(config-if)#ip address 192.168.99.99	(creates the router ID value)
RouterA(config-router)#exit	
RouterA(config)#interface fa0/0	
RouterA(config-if)#ip ospf cost 10	(set the OSPF cost)
RouterA(config)#interface fa0/1	
RouterA(config-if)#ip ospf cost 10	(set the OSPF cost)

Using wild cards on non 8 bit boundaries is dangerous. Use IP for each interface with 0.0.0.0 WC to avoid this problem.

Loopback interface
Use advertised = can be accessed across the network.
Use unadvertised = saves address space.

Show commands

show ip protocols	(show parameters for the router – timers, filters, metrics)
show ip ospf	(shows ospf settings and statistics ,times OSPF has been run)
show ip ospf neighbor	(shows neighbours)
show ip ospf neighbour *routerID*	(shows details for that neighbour)
show ip route ospf	(routing table OSPF details)
show ip ospf interface serial0	(shows OSPF details on that interface – timer intervals, hello intervals, neighbour adjacencies)
show ip ospf interface	(lists all interfaces in OSPF)

debug ip ospf events	(IP wrong, Hello/ dead intervals are wrong)
debug ip ospf packet	(captures log messages being sent and received)
debug ip ospf adj	(capture the authentication process and hello packet mismatches)
debug ip ospf hello	(captures hello messages)

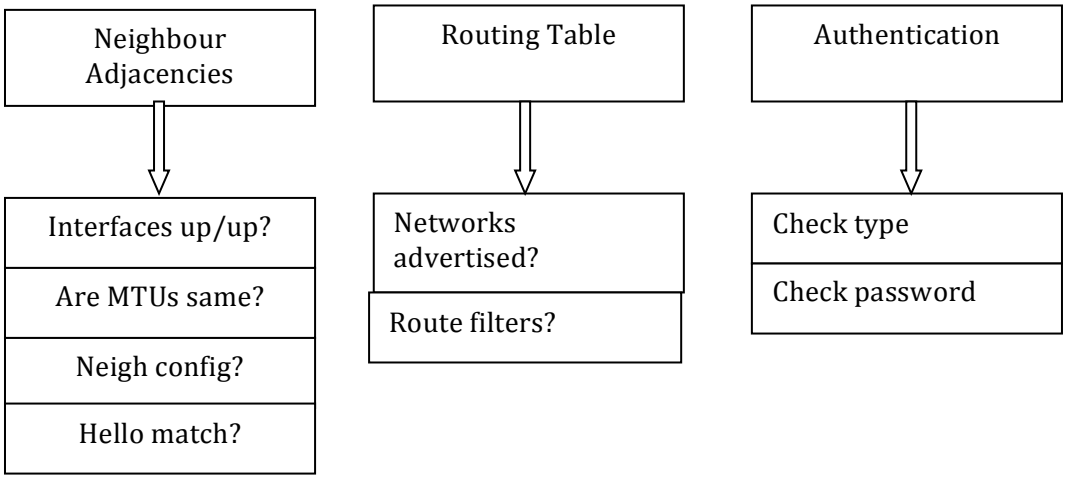
Authentication

RouterA(config)#interface fa0/1
RouterA(config-if)#ip ospf authentication-key *password*
RouterA(config-if)#ip ospf authentication
RouterA(config-if)#exit
RouterA(config-if)#router ospf 100
RouterA(config-router)#area 0 authentication

RouterA(config-if)#router ospf 100
RouterA(config-router)#area 0 authentication message-digest
RouterA(config-router)#exit
RouterA(config)# interface fa0/1
RouterA(config-if)#ip ospf message-digest-key 1 md5 cisco

Version 3
Advertises using multicast group FF02::5 (all OSPF routers) and FF02::6 (all OSPF designated routers)
Used link local addresses as the source

Troubleshooting



OPSF neighbour states

Down – no adjacency.
Attempt – Only on NBMA networks. Sends unicast Hello packets at Hello interval.
Init – Received HELLO packet, but it can't see itself in there.
2-way – It has been itself in the HELLO packet.
Exstart – DRs establish master slave relationship on segment and set starting numbers.
Exchange – send database info back and forth.
Loading – Link state info sent to those who need it.
Full – Full neighbour adjacency established. Neighbours have exchanged routes.

LSA types

1 – Generated for each Router for each area
2 – DR and BDR that describe a set of routers attached to a particular network.

ACLs

Ranges
Standard 1- 99 & 1300-1999 (expanded range)
Extended 100-199 & 2000-2699 (expanded range)

assess-list number {permit|deny} protocol source wc [port] dest wc [port] [established] [log]

protocols : IP, TCP, UDP, ICMP, GRE, IGRP

Creating a dynamic ACL
Step 1: Create a user authentication method on the router (local or remote)
Step 2: Define an extended ACL to permit vtp access but block all other traffic
Step 3: Create a dynamic ACL that applies to the extended ACL you created after it is authenticated.

RouterX(config)#username test password test
RouterX(config)#username test autocommand access-enable host timeout 10
RouterX(config)#access-list 101 permit tcp any host 10.1.1.1 eq telnet
RouterX(config)#interface fa0/0
RouterX(config-if)#ip address 10.1.1.1 255.255.255.0
RouterX(config-if)#ip access-group 101 in
RouterX(config-if)#exit
RouterX(config)#access-list 101 dynamic testlist timeout 15 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
RouterX(config)#line vty 0 4
RouterX(config-line)#login local

Creating a reflexive ACL

RouterX(config)#ip access-list extended outboundfilter
RouterX(config-ext-nacl)#permit icmp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
RouterX(config-ext-nacl)#permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 reflect tcptraffic
RouterX(config-ext-nacl)#exit
RouterX(config)#ip access-list extended inboundfilters
RouterX(config-ext-nacl)#permit icmp 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255 evaluate tcptraffic

RouterX(config-ext-nacl)#exit
RouterX(config)#int fa0/0
RouterX(config-if)#ip address 172.16.1.2 255.255.255.0
RouterX(config-if)#ip access-group inboundfilters in
RouterX(config-if)# ip access-group inboundfilters out

Creating a time based ACL

RouterX(config)#time-range EVERYOTHERDAY
RouterX(config-time-range)#periodic Monday Wednesday Friday 8:00 to 17:00
RouterX(config-time-range)#exit
RouterX(config)#periodic access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.161.0 0.0.0.255 eq telnet time-range EVERYOTHERDAY
RouterX(config)#int fa0/1
RouterX(config)#ip access-group 101 in

Configuring NAT

Configure static NAT
RouterA(config)#ip nat inside source static 192.168.10.5 216.1.1.3
RouterA(config)#int s0
RouterA(config-if)#ip nat outside (define s0 as connecting to the outside network)
RouterA(config-if)#int e0
RouterA(config-if)#ip nat inside (define e0 as connecting to the inside network)

Configure IPv6 DNS name servers
RouterA(config)#ip name-server *server-address1 [server-address2...server-address6]*

Configure PAT
RouterA(config)#access-list 20 permit 192.168.1.0 0.0.0.255 (define ACL)
RouterA(config)#ip nat inside source list 20 interface s0 overload (apply it to interface s0)

Nat pool
RouterA(config)# ip nat pool cisco 216.1.1.1 216.1.1.14 netmask 255.255.255.240
RouterA(config)# access-list 10 permit 192.168.10.0 0.0.0.255
RouterA(config)# ip nat inside source list 10 pool cisco

Show commands
Show ip nat translation (show NAT translation table)
Debug ip nat (shows natting process)

IP version 6

128 bits → 32 hexadecimal digital (as opposed to 32 binary digits!)

Advantages over IPv4
Larger address space – aggregation of prefixes.
Mobility and Security – IPSec is mandatory, Mobile IP is built in.
Translation Richness – Dual Stack, Tunnelling, NAT-PT

IPv6 has no broadcast!!! It uses multicast, unicast and Anycast (one-to-nearest ONLY ON ROUTERS)
Multicast uses FF00::/8

Types of Unicast addresses
Global – routable. Aggregated upwards to ISPs. 2003::/3
Reserved – IETF reserved for research.
Private (FE8 – FEF)
- Site to site – Site local. Routers forward within site but no to internet. FEC-FEF.
- Link-local – Refer to particular physical link. Refer only to particular segment. Automatic address configuration, neighbour discovery etc/

Loopback - ::1 test.
Unspecified – all zeros :: Refers to itself usually when asking for IP configuration.

Global unicast address
48-bit global routing prefix. 16-bit subnet ID (used by an organisation for subnets).

Address prefixing takes place to reduce the size of the routing table.

Interface identifiers
This is essentially the host portion. 64 bits. Can be assigned a number of ways:

Manually
Just like in IPv4.
RouterX(config-if)#ipv6 address 2001:DB8:222:7272::72/64

EUI-64

FFEE inserted into the middle of the interface's MAC address. 7th bit is set to 1 (global bit)
02 90 27 FF EE 17 FC 0F
RouterX(config-if)#ipv6 address 2001:DB8:0:1:: /64 eui-64

Stateless autoconfiguration
Determined from Router advertisements. It can be a while to wait so a node/device sends a solicitation messge asking for a router advertisement. This acts aS a plug and play feture and does not need a DHCP server.

DHCPv6
Updated version of v4.
-Can be used with Stateless
-Automatic DNS
-Looks at router advertisements to determine is DHCPv6 is used.
→ Send solicit → (DHCP) sends ALL-DHCPP-Agents-multicast with link local scope.
When it forwards a message it can send it to All-DHCP-Servers. You thus do not need to give a relay address like you do is DHCP v4. You can configure DHCP server to give out addresses based on different policies (i.e. don't give global IPs to printers).

ipv6 unicast-routing enables ipv6. Nothing will work beforehand. 12.2(2)T

Hostname configuration
ivp6 host *name [port] add1, add2 ... add4*. You can assign up to 4 IPv6 addresses for one hostname.
Ip name-server *dns add1 ... dns add6.*

RIPng
port 521 – FF02::9 multicast – modelled after v4.
RouterX(config)#ipv6 unicast-routing
RouterX(config)#ipv6 router rip EXAMPLENAME
RouterX(config)#interface Ethernet0
RouterX(config-if)#ipv6 address 2001:db8:1:1:::/64 eui-64
RouterX(config-if)#ipv6 rip EXAMPLENAME enable
RouterX(config)#interface Ethernet1
RouterX(config-if)#ipv6 address 2001:db8:1:2:::/64 eui-64
RouterX(config-if)#ipv6 rip EXAMPLENAME enable

Transitioning

Dual Stack

Node can use IPv4 and IPv6 (2 protocol stacks). Can configure on one or multipleinteraces. Chooses to use 4 or 6 based on destination address (prefers 6 where possible). New API is defined to support both (+ DNS req). Small change in source code of most apps will make it v6 compatible)

Tunneling

Protocol 41. 20-btye IPv4 header. Hard to troubleshoot. Decreases MTU. It is recommended to number tunnel endpoints.
Manual - IPv6 encapsulated in IPv4 – need dual stack
Dynamic 6to4 - IPv6 islands in an IPv4 network.
Intra-Site Automatic Tunnel Addressing Protocol - uses underlying IPv64 network as link layer for IPv6.
Teredo – host to host tunnelling (no router). Passes IPv6 unicast when NAT is between.

Proxy and Translation (NAT-PT)

Translate one type into another

Enabling an IPv6 tunnel

RouterA(config)# interface tunnel 0	(create the tunnel interface)
RouterA(config-if)# description IPv6 tunnel to Router A	(identify the tunnel)
RouterA(config-if)# ipv6 unnumbered ethernet 0	(use IPv6 address on e0 tunnel)
RouterA(config-if)# tunnel source ethernet 0	(set tunnel source as e0)
RouterA(config-if)# tunnel destination 192.168.10.2	(IPv4 address where tunnel ends)
RouterA(config-if)# tunnel mode ipv6ip	(IPv4 address where tunnel ends)

Virtual Private Networks

A VPN is an encrypted connection between private networks OVER a public network such as the internet. VPN uses IPSec to form virtual connections that are routed through the internet.

Type of VPNs

(1) Site to Site –
- Connects two whole networks to one another (i.e. site office to headquarters). Leased Line or Frame Relayed used to be used for this.
- Hosts do not have VPN client software
- They use a VPN gateway – router/firewall/ VPN concentrator/ASA5500
- It encapsulates, encrypts and sends over VPN tunnel (and vica versa)

(2) Remote access –
- Evolution of circuit switched networks (POTS ISDN)
- Supports Telecommuters, mobile users – Connects individual users.
- Used to use dial in. Now all they have to do is access the net.
- Client VPN client software IS needed.
- Sends data to VPN gateway.

Cisco Easy VPN

Has 2 parts:

(1) VPN Server/Gateway – Concentrator/PIX firewall/ASA adaptive security appliance/Cisco IOS router. Can terminate **Remote Access or site to site** VPNs (that use Cisco Easy VPN remote nodes).

(2) VPN remote clients – Can received security policies (thus minimising configurations). VPN parameters (Internet IP/SN/DHCP/WINS/split-tunnelling flags) can be pushed from the server to the remote device thanks to Cisco Easy VPN. Split tunnelling = you can access the internet at the same time that you are using the VPN.

Benefits:
- Dynamic config
- VPN config in INDEPENDENT of end user network details.
- Centralised security policy.
- Large scale deployment

Restrictions:

- No manual NAT or PAT – remote client does NAT/PAT for tunnel automatically.
- Only 1 destination peer/tunnel connection is supported.
- Requires destination servers – remote access servers needed.
- PSK and XAUTH are authentication. No Digital Certificates.
- Only ISAKMP are used – they use group 2 negotiation.
- Some transformation sets are not included (auth OR encrpy only = not supported)

IP Sec SSL VPN (Web VPN)

Uses web + native SSL encryption. SECURE ACCESS IS PROVIDED → REGARDLESS OF ENDPOINT HOST. No software client if the needs are modest.

Two methods of access: Clientless & Thin Client
Users can access – Files, Email, TCP Applications, without client software. Best for per-application users or access for privately own devices (laptops etc)

Benefits:

- Compatible with Dynamic Multipoint VPNs
- Compatible with Cisco firewalls
- Compatible with IPSec
- Compatible with Intrusion prevention systems
- Compatible with Cisco Easy VPN
- Compatible with NAT.

Restrictions:

- Supported only in software.
- The router CPU processes the WebVPN connections
- On-board VPN accelerates only IPSec.

Components of VPNs

Cisco provides VPN-enabled routers.

Cisco ASA5500 Series Adaptive Security Appliance:

- Provides remote access and site-to-site support
- Has IPSec and SSL VPN on one platform
- Also has firewall and IPS technology
- Remote access VPNs require one of the following 3 clients:

1. **Certicom** Client – Wireless PDA client

2. **Cisco VPN 3002 Hardware Client (legacy)** – Connect SOHO to VPN. 1 or 8 port switch version. Replaces SOHO PC applications.
3. **Cisco VPN Software client** – Software loaded onto PC. Can establish encrypted end-to-end tunnels. Cisco Easy VPN client can receive security config from Easy VPN server.

IPSec

Operates at the network layer. FRAMEWORK OF OPEN STANDARDS → can thus implement newer algorithms with having to designed the framework.

Encryption (digital scrambling)
data + encryption algorithm + key (string of digits) = unreadable cipher.
LONGER KEY = MORE SECURE
DH (Diffie-Helman) key agreement is a public key exchange. It allows 2 peers to establish a secret shared key even though it is over an insecure channel.

Encryption algorithms:
- **(1) DES (Data Encryption Standard) -** 56 bit key. Symmetric key.
- **(2) 3DES (Triple DES) -** Data is broken into 64 bit blocks. 3 different 56bit keys encrypt data one by one. Symmetric key.
- **(3) AES (Advanced Encryption Standard) -** Computationally better than 3DES. 128, 192 or 256 bit keys.
- **(4) RSA (Rivest, Shamir and Adleman) -** Asymmetrical key. 512+ in key length. IPSec doesn't use RSA. IKE uses it for peer authentication.

Integrity
Adds a hash to the method.
Transmitted hash = received hash = ☺
Message + Hash Algorithm + key = Message + hash value

HMAC (Hash Message Authentication Code) algorithms ***(these also authenticate)***:
(1) **MD5 (Message Digest 5)** - 128 bit shared key. Output is 128bit hash that is appended.
(2) **SHA-1 (Secure Hash Algorithm)** - 160 bit secret key. Output is 160bit hash that is appended.

Authentication
You are who you say you are.
Peer authentication methods:
(1) PSKs – manually entered into each peer. PSK + other info = key.
(2) RSA Signatures – exchanges digital certificates. Local end makes have with private key. Remote end makes hash with public key. Match = genuine.

Anti-replay protection
Verifies that there is no duplication. Compare seq # with receiver's sliding window. Outside window = late or duplicate = drop.

IPSec Protocol Framework – the two main protocols
AH (Authentication header): Authenticates, checks integrity. NO encryption.
ESP (encapsulating Security Payload): Authentication (for packet and ESP header) and encryption. Conceals payload and source/destination. One or the other must be selected.

IPSec protocol		ESP	AH	both
Encryption		DES	3DES	AES
Authentication		MD5	SHA	
DH		DH1	DH2	DH5

PPP

PPP is an encapsulation protocol for transporting IP traffic over point-to-point (leased line) serial connections. Frames are encapsulated before being sent over the WAN link. Synchronous and Asynchronous circuits.

Configuring PPP

- POTS (Asynchronous) / ISDN and Point-to-Point (Synchronous)
- LCP negotiates and sets up options (configures link).
- NCP carries packets from the network layer protocols.

Three phase setup process:

(1) Establish link – LCP packets sent back and forth. MTU units. Compression size. Authentication. Option not included = default assumed.
(2) Authentication PAP or CHAP.
(3) Network later protocol phase – NCP packets are sent to configure L3.

PAP – two way handshake. Repeatedly sends UN and PW until authentication or timeout. Passwords sent in plain text. No protection against repeated attempted. Remote node determines attempt freq.

CHAP – uses a 3 way handshake. Local Router sends a challenge to remote node. Remote node responds with one way hash function (MD5). Local router accepts or rejects. Challenges vary. Local router or authentication server is in determines freq.

Configuration:

(1) Enable PPP encapsulation.
(2) Enable authentication.

Enabling Authentication

(1) Give the router a name (hostname) – must match the username that the local router is expecting.
(2) Define the username and password on each router. There must been a username entry for each remote router.
(3) Pick an authentication . **ppp authentication {chap | pap | pap chap | chap pap}** If both are specified the first one mentioned will be tried first. IF peer suggests the second method or rejects the first the second is tried.

show interface (LCP Open means LCP has established a session)

debug ppp authentication ("by both" is two way chap authentication, I-incoming, O-outgoing, id field to match response with request)

Typical WAN protocols

HDLC (High-Level Data Link Control) – this is the default on point-to-point connections, dedicated links and circuit switched connections. It is a bit-oriented synchronous L2 protocol.

PPP (Point-to-Point Protocol) – Uses synchronous and Asynchronous circuits. Designed to work with higher levels like IP. Has PAP and CHAP.

Frame Relay – Switched L2 protocol that uses multiple VCs. No error correct or flow control.

ATM – 53-byte cell-switching. Video and Voice. Fixed length = fast processing.

Broadband – Two transmissions share a medium.

- DSL-PPPoE (encapsulates PPP in Ethernet frames) & PPPoA goes over the local telephone network. Auth. Encry. Compr.
- Cable-Ehternet uses a cable modem over cable TV infrastructure. 3Mbps – 30Mbps. Uses Ethernet frame.

Metro Ethernet – Point to Point and Multipoint services in business areas.

Frame Relay

Connection Oriented. Relies on upper layers for error correction. Frame Relay defines connection between router and Frame Relay Cloud edge. IT HAS NOTHING TO DO WITH HOW THINGS ARE ROUTED WITHIN THE FRAME RELAY CLOUD.

DTE – FRADs, routers and bridges. Owned by customer.

DCE – Provide clocking and switches. Transmits data through the WAN.

There are many VCs over a single connection. Connection IDs are assigned to DTE devices. Connection IDs are mapped to outbound ports in switching tables. Path to the destination is established before the first frame is sent.

Frame Relay Terms

Local access rate – clock speed of connection to frame relay cloud

VC – a logical circuit. DLCI is the identifier. Connects one DTE to another. Multiple VCs on one circuit.

PVC – No call setup/teardown. Always up.

SVC – dynamic/temporary.

DLCI – 10 bit connection VC identifier. LOCAL SIGNIFICANT. 2 dev = diff DLCI for same VC.

CIR (committed information rate) – Max average data rate that network tries to deliver. Specified when you subscribe. If you go over some frames are tagged as DE (discard eligible). CIR = 0 = all frames are DE.

Inverse ARP – Let a router find the IP address of a remote DTE based on the DLCI.

LMI (local management interface) – This is a signalling standard between the DTE and local Frame Relay switch (DCE). It manages the connection.

FECN (forward explicit congestion notification) – bit is set on the way to recipient DTE which passes it up to higher protocols for processing.

BECN (backward explicit congestion notification) – set in frames that travel in the opposite direction to frame with FECN bits set. This is so source DTE can learn of congestion.

Topology types – partial mesh, full mesh (all routers have VCs to other destinations. n(n-1)/2 links), star topology (most common frame relay topology).

FRAME RELAY NETWORK PROVIDES NBMA CONNECTIVITY BETWEEN REMOTE SITES. ALL ROUTERS ARE ON THE SAME SUBET.

NBMA are usually built into a hub and spoke topology. With a hub and spoke topology the physical setup does not have the multi-access capabilities that Ethernet does. This means that each router may not ne able to have separate PVCs to reach the other remote routers on the same subnet. This makes split horizon an issue because you have to run multiple PVCs over one network.

NMBA problems when using a single interface to interconnect multiple sites.

Routing updates: RouterA sends update to RouterCenter. RouterCenter cannot send the routing update out of the interface to other router (coz of the split horizon rule).

Solutions: Turn off split horizon. Not all network layers let you do this.

Use full mesh topology. Expensive.

Use sub-interfaces. Each VC can be considered a point-to-point connection. Each sub-interface can be on its own subnet.

Broadcast replication: If you have to broadcast out of one interface (to multiple remote devices) then you have to send multiple broadcasts out over the same link which can cause latency.

Each VC is mapped to a DLCI. Routers use LMI to find their local DLCI. They use ARP to find the remote IP based on their DLCI. Ie. Router figures out that DLCI 500 is associated with 10.1.1.1. If the router needs to talk to 10.1.1.1 it uses DLCI 500.

You can manually map DLCIs to IP addresses. Cisco routers try to auto detect the type of LMI that the frame relay router uses. Router sends out an LMI status request. Uses the latest that the switch sends back. Can also manually configure ty

LMI types: Cisco, ANSI and Q.933A

VC statuses

Active – can go ahead and exchange data.

Inactive – Connection to DCE ok. But remote router conection to DCE is not ok.
Deleted – no connection or LMI being received.

How Frame Relay works

1. Router connects to Frame Relay switch through CSU/DSU
2. Router sends LMI enquiry. Asks for connections status' of the routers VCs.
3. Frame Relay switch replies with local DLCIs of the VCs.
4. Router sends out IARP for each DLCI to introduce itself.
5. Remote router received IARP and makes an entry in its Frame Relay map table (IP→local DLCI)
6. IARPs are sent to all VCs every 60s LMI keepalives are sent to Frame Relay switch every 10s.
7. Router changes VC status based on LMIs from Frame Relay switch.

Configuring

RouterX(config)#interface serial1
RouterX(config-if)#ip address 10.16.0.1 255.255.255.0
RouterX(config-if)#encapsulation frame-relay [cisco|ietf] (use cisco for cisco)
RouterX(config-if)#frame-relay lmi-type [ansi|cisco|q933a] (11.2 or later autosenses)
RouterX(config-if)#bandwidth 64 (affects OSPF & EIGRP)
RouterX(config-if)#frame-relay inverse-arp ip 16 (protocol and DLCI – on by default)

No IARP → Frame Relay peers have different Frame Relay encapsulations. To control broadcast and multicast traffic you must manually map network to DLIC addresses.

RouterX(config-if)#frame-relay map *protovcol protocol-address dlci* [broadcast] [ietf|cisco|payload-compress packet-by-packet]

Broadcast allows broadcast and multicast over the VC. This lets you use dynamic routing protocol over the VC.

Payload-compress packet-by-packet enables a type of compression.

Sub-interfaces

Point-to-point: Each sub interface has a DLCI. Both ends on same subnet. Update traffic is no subject to split horizon.

RouterX(config)#interface serial0
RouterX(config-if)#no ip address
RouterX(config-if)#encapsulation frame-relay
RouterX(config-if)#interface serial0.110 point-to-point
RouterX(config-subif)#ip address 0.17.0.1 255.255.255.0
RouterX(config-subif)#bandwidth 64
RouterX(config-subif)#frame-relay interface-dlci 110
RouterX(config-subif)#interface serial0.120 point-to-point
RouterX(config-subif)#ip address 0.18.0.1 255.255.255.0
RouterX(config-subif)#bandwidth 64
RouterX(config-subif)#frame-relay interface-dlci 120 (must define to distinguish from phy)

DO NOT USE **frame-relay interface-dlci 120** ON PHYSICAL INTERFACES

Multipoint: The single multipoint sub interface has multiple PVCs. All on same subnet. Update traffic is subject to split horizon.

RouterX(config)#interface serial0
RouterX(config-if)#no ip address
RouterX(config-if)#encapsulation frame-relay
RouterX(config-if)#interface serial0.2 multipoint
RouterX(config-subif)#ip address 0.17.0.1 255.255.255.0
RouterX(config-subif)#bandwidth 64
RouterX(config-subif)#frame-relay map ip 10.17.0.2 120 broadcast
RouterX(config-subif)# frame-relay map ip 10.17.0.3 130 broadcast
RouterX(config-subif)# frame-relay map ip 10.17.0.4 140 broadcast (static mapping)
RouterX(config-subif)#no ip split-horizon (split horizon must be disabled to avoid problems)

IF YOU HAVE CONFIGURED THE SUBINTERACE AS MULTIPOINT AND IARP IS ENABLED YOU MUST CONFIGURE THE LOCAL DLCI FOR THE SUBINTERFACE TO DISTINGIUSH IT FROM THE PHYSICAL INTERFACE (I.E. BY TYPING frame-relay interface-dlci 120). YOU DO NOT NEED TO IN THE ABOVE EXAMPLE BAECAUSE YOU ARE STATICALLY MAPPING THE IPs TO THE DLCIs.

show interfaces

show frame-relay pvc
show frame-relay lmi
debug frame-relay lmi
show frame-relay map
clear frame-relay-inarp

Troubleshooting Frame Relay

Check the Frame Relay link – Use show interface serial to see of there is a layer 1 problem. Show controllers serial can show if the cable is present and correctly recognised.

To perform a loopback test:

1. Set encapsulation to hdlc and keepalive to 10s.
2. Set CSU/DSU to loopback mode.
3. If line protocol comes up the problem is beyond the CSU/DSU.
4. Ping is also useful (see page 349)

Incorrect DLCI can be wrong. Use the **show frame-relay pvc** command to check. If it shows as DELETED it could be configured wrong.
If interface = up. Line = down could be a L2 problem. Check with the **show frame-relay lmi** command.
NEXT... check the remote router

Check the remote router map **show frame-relay map**. If you have recently changed the interface on the remote frame relay router interface use the **clear frame relay-relay-inarp** command so that you do not have incorrect DLCI to IP mappings. If the remote router does not support IARP then maybe you need to statically map the DLCI and IPs. ACLs could be stopping the traffic from getting through. Temporarily disable it to see if this is the issue.

NEXT ... check end to end connectivity

Check the routing tables including the default gateway of the source node. If routing protocols are not working, you will need to check that broadcast traffic is supporting using the **show frame-relay map** command (if inverse ARP is configure broadcast is in effect automatically).

Administrative distances

Route Source	AD
Connected Route	0
Static Route	1
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200
Unknown	255

Private IP Ranges (RFC 1918)

10.0.0.0 to 10.255.255.255
172.16.0.0 to 172.31.255.255
192.168.0.0 to 192.168.255.255

Well-known Reserved Multicast addresses (non-exhuastive)

Multicast Route	Group Members
224.0.0.1	All Hosts
224.0.0.2	All Routers
224.0.0.5	All OSPF Routers
224.0.0.6	All OSPF DRs
224.0.0.9	All RIPV2 Routers
224.0.0.10	All EIGRP Routers

Connections from a host to a hub or from a hub to a switch must be half duplex because a hub is simply a repeater and does not guarantee a collision-free path.

Enabling port security (can only be done on an access port)
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-secuirty max 3
Switch(config-if)#switchport port-secuirty mac-addresss 1111.2222.3333
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation restrict