

Warsztaty CCNP

Cele szkolenia

Warsztaty CCNP przeznaczone są dla osób, które chcą poszerzyć swoją wiedzę z szerokiego zakresu sieci komputerowych w stosunku do zagadnień omawianych na kursie CCNA. Pomimo że implementacja omawianych zagadnień prezentowana jest na urządzeniach Cisco, to w większości przypadków same zagadnienia są uniwersalne, a poznaną wiedzę będzie można zastosować również w pracy z urządzeniami innych producentów. Certyfikat CCNP Enterprise to najpopularniejszy certyfikat potwierdzający znajomość zaawansowanych zagadnień sieciowych, a posiadanie go jest często wymaganiem koniecznym do dalszego rozwoju poważnej kariery sieciowej.

Umiejętności

Dzięki szkoleniu uczestnik będzie potrafił:

- Omówić zaawansowane protokoły sieciowe
- Poruszać się biegle w adresacji IPv4 i IPv6
- Skonfigurować przełącznik CISCO implementując zaawansowane zabezpieczenia i protokoły.
- Skonfigurować router CISCO – zaawansowane protokoły routingu,
- Automatyzować zarządzanie rozbudowaną infrastrukturą

Profil uczestników

Szkolenie przeznaczone jest głównie dla

- Inżynierów sieciowych wsparcia L2/L3
- administratorów systemów
- specjalistów IT
- specjalistów działów bezpieczeństwa

Przygotowanie uczestników

Uczestnicy powinny dysponować wiedzą z zakresu CISCO CCNA

Szczegółowy program szkolenia

1. Sieci VLAN, Trunki i technologia EtherChannel
 - a. Podstawowa konfiguracja wirtualnych sieci LAN
 - b. Trunki
 - c. Dynamic Trunking Protocol
 - d. VLAN Trunking Protocol (VTP) – wersje 1, 2 i 3
 - e. Protokoły drzewa opinającego
 - f. „Klasyczny” protokół drzewa opinającego (802.1d)
 - g. Per-VLAN Spanning Tree Protocol Plus (PVSTP+)
 - h. Rapid Spanning Tree Protocol (802.1w) oraz PVRST
 - i. Multiple Spanning Tree (802.1s)
 - j. Rozszerzenia protokołu Spanning Tree
 - k. BPDU Guard
 - l. BPDU Filtering/Root Guard
 - m. Loop Guard
 - n. UDLD/Routering w sieciach IP
2. Architektury i metody przełączenia pakietów
 - a. Wybór trasy, równoważenie obciążenia, trasy pływające i rekursywne
 - b. Routing statyczny w IPv4 i IPv6
3. Virtual routing and forwarding (VRF)
4. (Zaawansowane) protokoły wektora odległości i protokoły stanu łącza
 - a. Enhanced Interior Gateway Routing Protocol (EIGRP)
 - b. System autonomiczny, tablica sąsiadów, tablica topologii
 - c. Relacje sąsiedztwa, algorytm DUAL
 - d. Metryka, wybór trasy i równoważenie obciążenia
 - e. Podstawowa konfiguracja
 - f. Sumaryzacja
 - g. Uwierzytelnianie
 - h. Zbieżność i jej optymalizacja
5. Open Shortest Path First (OSPF)
 - a. Podstawy
 - b. Typy pakietów
 - c. ID routera
 - d. Relacja sąsiedztwa na łączach P2P i w sieciach LAN
 - e. Podstawowa konfiguracja
 - f. Typy sieci OSPF
 - g. Rodzaje LSA, obszary i ich rodzaje, propagacja LSA
 - h. Typy tras OSPF i wybór trasy
 - i. Sumaryzacja tras
 - j. Filtrowanie tras (z użyciem sumaryzacji, między obszarami oraz lokalne)
 - k. OSPFv3 dla IPv6
 - l. Obsługa IPv4 w OSPFv3
6. Border Gateway Protocol (BGP)
 - a. Czy i kiedy potrzebujemy BGP?

- b. Multihoming
 - c. Wewnętrzne i zewnętrzne sesje BGP
 - d. Tablica BGP
 - e. Atrybuty trasy i algorytm wyboru trasy
 - f. Podstawowa konfiguracja BGP (sąsiedzi i rozgłaszanie tras)
 - g. Zarządzanie relacjami sąsiedztwa
 - h. Algorytm wyboru trasy
 - i. Kwestie bezpieczeństwa
 - j. Inżynieria ruchu i manipulacja atrybutami BGP
 - k. Filtrowanie aktualizacji (ACL, prefix-list, AS-path ACL)
 - l. Zastosowanie Route-map w BGP
 - m. Sumaryzacja tras (atrybuty atomic aggregate i AS_SET)
 - n. BGP Communities
 - o. Multi-protocol (MP) BGP i obsługa IPv6
7. First Hop Redundancy Protocols (FHRP)
- a. Hot Standby Router Protocol (HSRP)
 - b. Virtual Router Redundancy Protocol (VRRP)
 - c. Gateway Load Balancing Protocol (GLBP)
8. Translacja adresów sieciowych
9. Tunelowanie ruch – sieci nakładkowe
- a. Podstawy IPSec
 - b. Tunele Generic Routing Encapsulation (GRE) bezpieczne tunele GRE
 - c. Location ID Separation Protocol (LISP)
 - d. Virtual Extensible LAN (VXLAN)
10. Sieci bezprzewodowe
- a. Częstotliwości, długość, moc fal elektromagnetycznych
 - b. Przesyłanie danych w sieciach bezprzewodowych
 - c. Asocjacja klienta z AP
 - d. WEP, WPA, WPA2, WPA3
 - e. EAP
11. Podstawowa diagnostyka – ping/traceroute
12. Używanie narzędzi debug
13. Syslog/SNMP
14. Switched Port Analyzer (SPAN)
15. IP SLA i object tracking
16. Listy kontroli dostępu
- a. Standardowe/rozszerzone
 - b. Numerowane/nazwane
 - c. Port ACL
 - d. VLAN ACL
 - e. Router ACL
17. Telnet/SSH
18. AAA new model
19. Zone-Based Firewall (ZBFW)
20. Automatyzacja sieci z Ansible

Metoda realizacji szkolenia

Wykłady i ćwiczenia praktyczne

Liczba dni, liczba godzin szkoleniowych

5 dni, 40 godzin szkoleniowych

Ścieżka rozwoju po szkoleniu

Zapraszamy na pozostałe szkolenia z naszej oferty dotyczącej <https://www.comarch.pl/szkolenia/systemy-operacyjne-i-sieci-komputerowe/>