Ostrowiec Św., dnia 20.12.2021r.

Znak sprawy: ZP.271.3.10.2021

ZAMAWIAJĄCY Powiat Ostrowiecki - Dom Pomocy Społecznej
os. Słoneczne 49, 27-400 Ostrowiec Św.
tel. 41 266 55 53 , fax: 41 263 51 81
strona internetowa: www.dpsostrowiec.pl
e-mail : sekretariat@dpsostrowiec.pl

Wyjaśnienie treści do Zapytania ofertowego

„Usługa ochrony fizycznej obiektu, osób, mienia i terenu Domu Pomocy Społecznej w Ostrowcu Św., os. Słoneczne 49 wraz z obsługą portierni i zapewnieniem reakcji grupy interwencyjnej w 2022 roku.”

Postępowanie jest prowadzone na podstawie Regulaminu udzielania zamówień publicznych o wartości poniżej 130 000 zł netto wprowadzonego zarządzeniem Nr 4/2021 Dyrektora Domu Pomocy Społecznej w Ostrowcu Św. os. Słoneczne 49 z dnia 12.01.2021 r.

Pytanie 1:

Jaki wpływ na jakość świadczonej usługi ma odległość pomiędzy siedzibą Wykonawcy a miejscem wykonywania usługi? Z jakiego powodu została ona zawężona do 10 km, a nie np.: do 20 km ? W istotny sposób ogranicza się liczbę potencjalnych Wykonawców a tym samym sprawia, że zmniejsza się konkurencja cenowa wśród podmiotów zainteresowanych świadczeniem w/w usługi, ze szkodą dla Zamawiającego?

Odpowiedź:

Zamawiający ustalił odległość 10 km mając na względzie specyfikę placówki i tym samym szybki przyjazd grupy interwencyjnej na zgłoszenie.

Pytanie 2:

Czym Zamawiający uzasadnia wymaganie posiadania przez pracowników ochrony uprawnień SEP do 1 kW, jeśli z treści zapytania nie wynika, że mają oni dokonywać czynności naprawczych lub instalatorskich, do których wymagane są powyższe uprawnienia?

Odpowiedź:

Zamawiający wymaga przedmiotowych uprawnień do szybkiej reakcji usuwania awarii w czasie świadczenia usługi przez pracowników ochrony szczególnie podczas pełnienia dyżurów w porze nocnej i w dni świąteczne.

Pytanie 3:

Jakie parametry techniczne ma spełniać „platforma”? Jakiego typu ma to być urządzenie, jaka charakterystykę pracy posiadać, jakie normy spełniać?

Odpowiedź:

Urządzenia o jakich mowa w zapytaniu ofertowym to m.in. serwery spełniające rolę stacji odbierającej sygnały (alarmowe, o stanie systemu i inne), nadawane przez urządzenia – nadajniki, wysyłające wspomniane sygnały za pomocą przedmiotowego protokołu IP, drogą GSM i poprzez urządzenia radiowe.
Zamawiający poniżej przedkłada wyjaśnienia dotyczące infrastruktury technicznej umożliwiającej zarządzanie zabezpieczeniami opartymi na protokole IP, o jakie chodzi w prowadzonym postępowaniu o udzielenie zamówienia na ww. usługę.

Format pakietu IPv4

Pakiet IP składa się z nagłówka oraz danych. Ze względów technicznych pakiet ten został przedstawiony w formie tabelarycznej, po 32 bity (4 bajty) w rzędzie. Natomiast w rzeczywistości należy go sobie wyobrazić jako jednolity strumień bitów przedstawionych w sposób ciągły. Poszczególne pola pakietu mają następujące znaczenie: - wersja (VERS) - pole 4-bitowe określające typ protokołu IP. Jeśli jest tam wpisana wartość 4 oznacza to wersję czwartą protokołu. Jeśli jest tam wartość 6 oznacza to IPv6. Rozróżnianie pomiędzy pakietami wersji 4 i 6 jest przeprowadzane już przy analizowaniu ramki warstwy drugiej poprzez badanie pola typu protokołu. długość nagłówka (HLEN) - pole 4 bitowe określające długość datagramu wyrażoną jako wielokrotność słów 32 bitowych. typ usługi (TOS ang. Type-of-Service) - 8-bitowe pole określające poziom ważności jaki został nadany przez protokół wyższej warstwy. Znaczenie poszczególnych bitów tego pola jest następujące: pierwsze 3 bity: wartość 0 - stopień normalny, wartość 7 - sterowanie siecią czwarty bit - O - prośba o krótkie czasy oczekiwania piąty bit - S - prośba o przesyłanie danych szybkimi łączami szósty bit P - prośba o dużą pewność przesyłania danych bity 6, 7 nieużywane całkowita długość - pole 16-bitowe. Długość całego pakietu wyrażona w bajtach. W celu uzyskania długości pola danych należy odjąć od długości całkowitej długość nagłówka. Wartość minimalna wynosi 576 oktetów zaś maksymalna 65535 oktetów, tzn. 64 kB Identyfikacja - 16 bitowe pole używane do określania numeru sekwencyjnego bieżącego datagramu. Znaczniki - 3 bitowe pole. Pierwszy najbardziej znaczący ma zawsze wartość 0. Kolejne znaczące bity sterują fragmentacją (0- oznacza, czy pakiet może zostać podzielony na fragmenty, 1 - nie może być podzielony). Trzeci bit oznacza: ostatni pakiet powstały w wyniku podzielenia (jeśli ma wartość 1) lub pakiet ze środka 0. Przesunięcie fragmentu - 13-bitowe pole służące do składania fragmentów datagramu. Czas życia (TTL, ang. Time To Live) - 8-bitowe pole określające liczbę routerów (przeskoków), przez które może być przesłany pakiet. Wartość tego pola jest zmniejszana przy przejście przez każdy router na ścieżce. Gdy wartość tego pola wynosi 0, wtedy pakiet taki jest odrzucany. Zasada ta pozwala na stosowanie mechanizmów zapobiegających zapętlaniu się tras routingu. Protokół - 8-bitowe pole określające, który z protokołów warstwy wyższej odpowiada za przetworzenie pola Dane. Możliwe opcje tego pola zostały przedstawione na następnych slajdach. Suma kontrolna nagłówka - 16-bitowe pole z sumą kontrolną nagłówka pozwalającą stwierdzić, czy nie nastąpiło, naruszenie integralności nagłówka. Ze względu na fakt, że każdy router dokonuje zmian w nagłówku musi ona być przeliczona na każdym z routerów. Adres IP nadawcy - 32-bitowe pole z adresem IP nadawcy pakietu Adres IP odbiorcy - 32-bitowe pole z adresem IP odbiorcy pakietu Opcje - pole to nie występuje we wszystkich pakietach. Szczegółowe wartości tego pola zostaną omówione na następnym slajdzie.

Uzupełnienie (Wypełnienie) - pole to jest wypełnione zerami i jest potrzebne, żeby długość nagłówka była wielokrotnością 32 bitów (patrz-> Długość nagłówka) Dane - pole od długości do 64kB zawierające dane pochodzące z wyższych warstw.

Protokół ICMP

Tak jak już zostało to wcześniej wspomniane sam protokół IP nie sprawdza, czy dane dotarły do adresata.
Z tego punktu widzenia jest określany jako protokół zawodny. Rolę sprawdzania, czy pakiety docierają do adresata pełnią protokoły wyższych warstw.
W ramach warstwy sieciowej sprawdzaniem dostępności sieci docelowej zajmuje się protokół ICMP (ang. Internet Control Message Protocol). Jego zadaniem nie jest rozwiązywanie problemów z zawodnością IP, ale zgłaszanie braku łączności. Protokół ten został zdefiniowany w dokumencie RFC 792.
Komunikaty ICMP wysyłają zwykle bramy lub hosty. Najczęstsze powody wysyłania tych komunikatów to: zbytnie obciążenie routera lub hosta - wysyłany jest komunikat ICMP, że należy zwolnić prędkość przesyłania komunikatów, bo host nie nadąża je przetwarzać router lub host znajduje lepszą trasę - może wtedy wysłać do źródła komunikat o lepszej trasie host docelowy jest nieosiągalny - wtedy ostatnia brama wysyła komunikat

ICMP o niedostępności adresata i przesyła go do hosta źródłowego pole TTL pakietu jest równe 0 - wtedy router może wysłać komunikat ICMP do źródła i odrzuca pakiet.

Dostarczanie komunikatów ICMP

Przy przesyłaniu komunikaty ICMP są poddawane enkapsulacji do postaci pakietów IP, a następnie do postaci ramki warstwy drugiej. Pod tym względem stanowią one integralną część danych pakietu IP. Jak zostało to pokazane na rysunku, sam komunikat ICMP jest przesyłany w datagramie IP. Komunikat ICMP składa się z nagłówka ICMP oraz danych ICMP. Warto przy tym zauważyć, że ze względu na zawodny charakter protokołu IP w momencie zaginięcia datagramu przenoszącego komunikat ICMP nie zostanie to zdiagnozowane. Wysyłanie komunikatów o błędach powodowałoby występowanie znacznego ruchu w sieci.
Struktura datagramu ICMP jest odmienna od struktury datagramu IP. Wspólny jest tylko sposób adresacji.

Format komunikatu ICMP

Najważniejsze dane przesyłane w komunikacie ICMP zawarte są w polach TYP i KOD. Zatem wszystkie wersje komunikatów ICMP musza zawierać pola: Typ, Kod, Suma kontrolna. Znaczenie poszczególnych bajtów jest następujące:
Pole Typ: 0 - odpowiedź z echem (ang. Echo Reply) 3 - odbiorca nieosiągalny (ang. Destination Unreachable). 4 - zmniejszenie szybkości nadawania - tłumienie źródła (ang. source quench) 5 - zmiana trasowania - przekierowanie (ang. redirect). 8 - prośba o echo (ang. echo request) 9 - rozgłaszanie routera (ang. router advertisement) 10 - wywołanie routera (ang. router solicitation) 11 - przekroczenie TTL (ang. Time Exceeded) 12 - kłopot z parametrami datagramu 13 - prośba / żądanie o wysłanie znacznika czasu (ang. timestamp request) 14 - odpowiedź na prośbę / żądanie o wysłanie znacznika czasu (ang. timestamp reply) 15 - prośba o informację 16 - odpowiedź z informacją 17 - prośba o maskę adresu 18 - odpowiedź z maską adresu 30 - Traceroute 31 - błąd konwersji datagramu (ang. Datagram Conversion Error) 32 - przekierowanie hosta mobilnego (ang. Mobile Host Redirect) 33 - IPv6 Where-Are-You 34 - IPv6 Here-I-Am 35 - prośba o zarejestrowanie urządzenia mobilnego (ang. Mobile Registration Request) 36 - odpowiedź na prośbę o zarejestrowanie urządzenia mobilnego (ang. Mobile Registration Reply) 37 - żądanie nazw domeny (ang. Domain Name Request) 38 - zwrot nazwy domeny (ang. Domain Name Reply) 39 - SKIP Algorithm Discovery Protocol 40 - Photuris, Security Failures

W zależności od wartości występującej w polu Typ, wartość pola Kod może zawierać różne liczby. Najczęściej spotykane wartości par Typ, Komunikat zostaną przedstawione na następnych slajdach. Następujące wartości pola Typ są zarezerwowane : 1,2,7,19 (zarezerwowane dla bezpieczeństwa), 20-29, 41-255.

Kmounikaty: echo request i echo response

W przypadku komunikatu ICMP typu żądanie echa (ang. echo request) i odpowiedzi z echem (ang. echo reply) wartości pola typ wynoszą odpowiednio 8 albo 0. Wartość pola Kod w obu przypadkach wynosi 0. Dodatkowo w celu połączenia zapytań i odpowiedzi pola Identyfikator i Numer sekwencyjny muszą mieć wartości unikalne. W polu danych mogą być przenoszone dodatkowe informacje potrzebne do zapytania i/lub odpowiedzi.
Tego typu komunikaty ICMP są wykorzystywane przez podstawowe programy testujące, takie jak ping czy traceroute. Przykłady wywołania tych programów zostaną podane na kolejnych slajdach.

Komunikat ICMP destination unreachable

Przy próbach wysyłania pakietów do miejsca przeznaczenia może wystąpić szereg błędów związanych z np. z uszkodzeniem łącza, błędnym adresem docelowym, nieznaną lokalizacją, itd. W takich przypadkach router, który wykryje problem wysyła komunikat o niedostępnym adresacie (ang. destination unreachable) w postaci przedstawionej na rysunku. W zależności od przyczyny błędu w polu „Kod" pojawiają się wartości liczbowe powiązane z następującymi usterkami: 0 - sieć niedostępna 1 - host niedostępny 2 - protokół niedostępny 3 - port niedostępny 4 - niezbędna fragmentacja, ustawiona wartość DF 5 - nie powiodło się określenie trasy przez nadawcę (ang. source route) 6 - nieznana sieć docelowa 7 - nieznany host docelowy 8 - host źródłowy odizolowany 9 - komunikacja z siecią docelową zablokowana przez administratora 10 - komunikacja z hostem docelowym zablokowana przez administratora 11 - sieć niedostępna dla tego typu usługi 12 - host niedostępny dla tego typu usługi

Komunikat o niedostępnym adresie wysyłany jest również w przypadku, gdy przesyłany pakiet musi zostać podzielony na mniejsze datagramy, np. przy przesyłaniu z sieci typu Token Ring do sieci Ethernet, a znacznik w nagłówku pakietu nie pozwala na taką fragmentację. Wysyłany jest wtedy kod błędu o wartości 4. W przypadku zablokowania przez administratora określonych usług sieciowych, takich jak np. www, również nie można przesłać pakietów z żądaniem wyświetlenia strony. Generowany jest wtedy komunikat o niedostępnym adresacie ze stosowną wartością kodu błędu.

Narzędzia diagnostyczne wykorzystujące ICMP

Komunikaty ICMP są wykorzystywane przez program narzędziowy ping. Program ten wysyła komunikat ICMP z wartością pola Typ ustawioną na wartość równą 8 prośba o wysłanie komunikatu echo (ang. echo request). W odpowiedzi na ten komunikat host, do którego jest adresowany ten komunikat może odpowiedzieć komunikatem ICMP o wartości pola Typ równą 0.
Innym powszechnie stosowanym programem narzędziowym jest program traceroute. Przykład efektu wywołania tego programu został przedstawiony na slajdzie.

Komunikat ICMP: problem związany z parametrem

Kolejnym przykładem błędu powodującego wysłanie komunikatu ICMP jest sytuacja, gdy w nagłówku przesyłanego pakietu są błędy. Wysyłany jest wtedy komunikat błędu o postaci takiej jak na slajdzie, z wartością pola Typ równą 12. Błąd ten oznacza, że jest problem związany z parametrem (ang. parameter problem).
Jeśli pole „Kod" ma wartość 0, to wartość w polu „Wskaźnik" wskazuje numer oktetu nagłówka datagramu, w którym występuje błędna wartość parametru.

Komunikaty sterujące ICMP

Oprócz komunikatów o błędach, które zostały częściowo omówione na poprzednich slajdach protokół ICMP służy również do przesyłania komunikatów sterujących (stąd część nazwy protokołu: control). Komunikaty te są wysyłane, m.in. w celu efektywniejszego przesyłania pakietów przez IP.

Komunikat ICMP: tłumienie źródła

W przypadku, gdy host nie nadąża z przetworzeniem pakietów to wysyłany jest komunikat ICMP z kodem „Typ" równym 4, oznaczający tłumienie źródła (ang. source quench). Sytuacja taka ma zwykle miejsce, gdy jeden z komputerów otrzymuje pakiety z wielu źródeł. Zwykle w takich przypadkach zmniejszana jest wielkość okna TCP.W przykładzie na rysunku pokazany jest przypadek wysłania komunikatu tłumienia źródła przez router, który jest połączony z dostawcą Internetu przy pomocy łącza o niewielkiej przepustowości (np. 100 Mb), zaś sieć lokalna pracuje z wyższą prędkością.

Komunikat ICMP: zmiana trasowania / przekierowanie

Jednym z komunikatów sterujących ICMP jest komunikat zmiany trasowania / przekierowania.

W przykładzie zamieszczonym na rysunku host H1, o numerze IP 192.168.1.10/24, chce przesłać pakiet do hosta H2 o numerze IP 10.1.2.10/8. Host H1 ma ustawioną bramę domyślną o adresie 192.168.1.1/24 i do niej mógłby wysyłać pakiety skierowane do hosta H2. Jednak pakiety te wysłane na interfejs E0 routera A będą przez ten router kierowane na ten sam interfejs i wysyłane do routera B, który następnie będzie przesyłał dalej do hosta H2. Aby uniknąć niepotrzebnego przesyłania pakietów przez router A urządzenie to prześle komunikat ICMP do hosta H1, żeby przyszłe pakiety do hosta H1 oraz sieci 10.1.2.0/8, wysyłał na adres routera B (192.168.1.2/24).. I tak w przypadku wykrycia lepszej trasy dla pakietów wysyłany jest komunikat o wartości pola Typ równej 5. Oznacza on zmianę trasowania / przekierowanie (ang. redirect). Za wysłanie takiego komunikatu odpowiada host będący domyślną bramą, żeby komunikat taki został wysłany muszą być jednak spełnione następujące warunki: - pakiet przesyłany do routera na jego interfejs jest następnie zawracany i kierowany przez ten sam interfejs do innego routera - adres sieci IP nadawcy jest taki sam jak routera następnego przeskoku routowanego pakietu - trasa pakietu nie jest określona przez nadawcę - trasa określona po przekierowaniu nie jest trasą domyślną lub kolejnym przekierowaniem ICMP - router jest skonfigurowany do wysyłania żądań przekierowania pakietów.

Żądanie przekierowania pakietów w zależności od wartości pola Kod może dotyczyć zarówno sieci jak i hostów: - 0 - datagramy przekierowania dla sieci - 1 - datagramy przekierowania dla hosta - 2 - datagramy przekierowania dla typu usługi i sieci - 3 - datagramy przekierowania dla typu usługi i hosta W polu „adres internetowy routera" (ang. Router Internet Address) wskazywany jest adres urządzenia, które będzie pełniło bramę dla pakietów przesyłanych do sieci, dla których zostało wygenerowane żądanie przekierowania.

Komunikat ICMP: żądanie znacznika czasu

Przy komunikacji poprzez sieci rozległe może istnieć potrzeba synchronizacji zegarów w odległych od siebie lokalizacjach. Ma to istotne znaczenie w przypadku użytkowania aplikacji wymagających zgodności znaczników czasowych.
W celu synchronizacji zegarów na danym hoście (serwerze) z innym hostem (serwerem) wysyłany jest stosowny komunikat ICMP żądanie / prośba wysłania znacznika czasowego (ang. timestamp request) o wartości pola Typ równej 13. W odpowiedzi na taką prośbę wysyłany jest komunikat odpowiedzi o wartości pola Typ równej 14. Pola kodu w przypadku obu typów komunikatów są równe 0. Pola, w których będą umieszczane znaczniki czasu są wypełniane czasem podanym w milisekundach liczonych od północy czasu uniwersalnego (UTC). Przed wysłaniem komunikatu wypełniane jest pole „Początkowy znacznik czasu" wartością daty i godziny czasu dla hosta źródłowego. W polu „Znacznik czasu odbioru" wstawiany jest czas odbioru przez host docelowy komunikatu z żądaniem wysłania znacznika czasu. Następnie, przed wysłaniem komunikatu z odpowiedzią, wypełniany jest aktualny czas do pola „Znacznik czasu wysłania".
Analiza trzech pól przesłanych w odpowiedzi na prośbę o znacznik czasu umożliwia oszacowanie czasu przesyłania pakietu przez sieć zarówno w jedną jak i drugą stronę. W praktyce zamiast tego typu pomiarów stosuje się protokoły wyższych warstw stosu protokołów TCP/IP, np. protokół NTP (ang. Network Time Protocol).

Komunikat ICMP: żądanie przesłania informacji

Komunikaty żądanie / prośba o przesłanie informacji (ang. information request) oraz odpowiedź na żądanie przesłania informacji (ang. information reply) zostały zaprojektowane z myślą o przesyłaniu numerów IP. W zależności od tego czy jest to prośba o informację, czy też odpowiedź na tę prośbę pole Typ ma wartości: 15 lub 16. W przypadku obu typów komunikatów wartości pola „Kod" wynoszą 0.
W praktyce obecnie nie są wykorzystywane, gdyż informacje takie są przesyłane w sposób bardziej dogodny przez protokoły takie jak BOOTP, RARP czy też DHCP. Protokoły służące uzyskiwaniu adresów zostaną omówione w kolejnym module poświęconym automatycznemu uzyskiwaniu adresów IP.

Komunikat ICMP: żądanie maski adresu

Komunikat ICMP typu żądanie maski adresowej oraz odpowiedź na żądanie maski adresowej mają odpowiednio wartości pól Typ wypełnione liczbami 17 i 18. Komunikaty te służą określeniu przez hosta jego maski adresowej.
W przypadku, gdy host zna adres routera w danej podsieci, komunikat żądanie maski adresowej wysyłany jest na adres tego komputera. W przeciwnym razie komunikat ten wysyłany jest na adres rozgłoszeniowy. W odpowiedzi router wysyła na adres hosta, który wysłał żadanie, netmaskę w odpowiednim polu komunikatu zwrotnego.
Pola „Identyfikator" jak i „Numer sekwencyjny" służą do skojarzenia zapytań i odpowiedzi.
Mogą mieć wartość 0.

IRDP: Komunikaty ICMP umożliwiające wykrywanie routera

Komunikaty służące do wykrywania routera (ang. router discovery messages) są pomocne w momencie podłączania do sieci hosta, który nie ma wpisanego w sposób statyczny adresu routera. Komunikaty takie są wykorzystywane przez protokół IRDP (ang. ICMP Router Discovery Protocol), który działa w oparciu o protokół ICMP. Pozyskanie takiego adresu, przy pomocy protokołu IRDP, poprzez nowo podłączony host może odbyć się w dwojaki sposób.
Jednym z nich jest cykliczne wysyłanie przez router komunikatów rozgłaszania routera (ang. router advertisement), które mogą zostać odebrane przez hosty w sieci lokalnej. Komunikat taki ma w polu Typ wpisaną wartość 9. Komunikaty rozgłaszania routera nie służą do wyboru najlepszego routera do przesyłania pakietów do określonej lokalizacji. Gdy host wybierze router, który nie jest optymalny do przesyłania pakietów

do określonej lokalizacji, to powinien zostać o tym poinformowany poprzez komunikat ICMP o przekierowaniu (komunikat ten został omówiony na jednym z wcześniejszych slajdów.
Drugim sposobem jest wysłanie przez nowo podłączony do sieci host komunikatu wywołania routera (ang. router solicitation). Taki komunikat ma w polu Typ wpisaną wartość 10.
Wyżej wymienione typy komunikatów zostaną przedstawione na kolejnych slajdach. Należy podkreślić, że ze względu na własności protokołu DHCP (zostanie on omówiony w module poświęconym automatycznemu pozyskiwaniu adresów IP) znaczenie protokołu IRDP jest obecnie niewielkie.

Komunikaty ICMP: rozgłaszanie routera

Komunikat rozgłaszania routera został przedstawiony na slajdzie. Poszczególne pola mają następujące znaczenie:
Liczba adresów - liczba adresów przesyłana w tym komunikacie
Rozmiar pozycji adresu - liczba 32 bitowych słów przeznaczonych na pole adresu routera(ów).
Czas życia - czas w sekundach, przez który adresy routerów przesłane w komunikacie są aktualne. Domyślna wartość wynosi 30 min.
Adres routera - adres routera
Poziom preferencji - pole umożliwiające oznaczenie przez administratora routera, który jest bardziej predestynowany do danej funkcji. Wartość tego pola waha się w granicach 1 do „Liczby adresów. Czym wyższa wartość tego pola tym wybór tego routera jest bardziej pożądany.

Komunikaty ICMP: wywołanie routera

Jeśli host nie ma ustawionej domyślnej bramy to wysyła komunikat wywołania routera (ang. router solicitation). Komunikat ten jest wysyłany na adres grupowy 224.0.0.2. Jeśli komunikat ten zostanie odebrany przez router z działającą procedurą wykrywania routera, to odpowie komunikatem przedstawionym na poprzednim slajdzie.

Protokół IGMP

Protokół zarządzania grupami internetowymi IGMP (ang. Internet Group Menagement Protocol) został opracowany z myślą o dogodnej komunikacji urządzeń sieciowych przy pomocy transmisji grupowych. Działanie tego protokołu jest trochę podobne do komunikacji przy pomocy kanałów telewizyjnych lub radiowych, albo jeszcze lepiej krótkofalarskich. Klient decyduje do którego kanału się podłącza (jaki program go interesuje) i tylko te informacje otrzymuje jak również do tego samego kręgu zainteresowanych stacji kieruje swoje komunikaty. Standard tego protokołu został opublikowany w dokumencie RFC 1112 pod koniec lat 90-tych XXw.
Działanie takie jest możliwe, dzięki transmisjom grupowym (ang. multicasting). W tym typie transmisji pakiety wysyłane są na adres grupowy IP. Routery wiedzą, które komputery znajdują się w grupie obsługiwanej przez daną aplikację. Pozwala to na jednokrotne wysłanie określonych danych do wszystkich hostów z danej grupy. Jest to działanie bardziej efektywne niż transmisje kierowane (ang. unicasting), czy też wysyłanie poprzez adres rozgłoszeniowy (ang. broadcasting).

IGMP: typy komunikatów

Hosty, które chcą się przyłączyć do danej grupy wysyłają komunikat IGMP Host Membership Report. Przyłączenie się klienta do danej grupy składa się z dwóch procesów:
-host powiadamia router o tym, że chce się przyłączyć do danej grupy -host wiąże w sposób dynamiczny IP z adresem grupowym, który jest zarezerwowany dla danej aplikacji oraz z zarezerwowanym adresem Ethernetowym.
Opuszczenie danej grupy odbywa się poprzez wysłanie komunikatu IGMP Explicit Leave. Host powinien powiadomić lokalne routery o zamiarze opuszczenia grupy poprzez wysłanie właśnie takiego komunikatu. Routery okresowo sprawdzają czy w dalszym ciągu istnieje potrzeba przesyłania pakietów na adres grupowy. Kontrola taka odbywa się poprzez wysłanie zapytania przy użyciu adresu grupowego przeznaczonego dla wszystkich hostów (224.0.0.1). Pakiety które są wysyłane pod ten zarezerwowany numer IP mają ustawione pole TTL na wartość jeden, dzięki temu nie są rozsyłane dalej przez inne routery. W odpowiedzi hosty powinny przesłać pakiet raportu z adresem takim jaki jest zarezerwowany dla tej grupy. Po sprawdzeniu, które z grup jeszcze istnieją routery będą przesyła tylko pakiety dla funkcjonujących grup, natomiast pakiety z adresem grupowym będą odrzucane przez router.

IGMP: struktura pakietu

W nagłówku pakietu IGMP przesyłane są następujące pola:
Wersja - 4b - wersja pakietu IGMP Typ - 4b - typ komunikatu. Wartości tam zapisane oznaczają odpowiednio;

1 - zapytanie o przynależność hosta
2 - raport o przynależności hosta

Nie używane - 8b - pole nie wykorzystywane Suma kontrolna - 16b - pole wykorzystywane do przesyłania liczby umożliwiającej sprawdzenie integralności pakietu Adres grupy - 32b - gdy pakiet jest przesyłany w celu zapytania o przynależność hosta, to pole to jest puste. Gdy host odpowiada raportem o przynależność do grupy, to w polu tym przesyłany jest adres rozsyłania grupowego konkretnej grupy.

IGMP: współpraca z innymi protokołami rozsyłania grupowego

Protokół IGMP obsługuje rozsyłanie grupowe wewnątrz sieci lokalnych. Przesyłaniem pakietów grupowych pomiędzy routerami zajmują się grupowe protokoły trasowania (ang. Multicast Router Protocol).
Wśród najczęściej spotykanych protokołów rozsyłania grupowego działających pomiędzy routerami sa: PIM (ang. Protocol Independent Multicast Protocol) - protokół adresowania grupowego niezależny od protokołów. Standard ten został opisany w dokumencie RFC 2117. MOSPF (ang. Multicast Extensions to OSPF) - rozszerzenie protokołu OSPF o adresowanie grupowe. Protokół ten został opisany w dokumencie RFC 1584 DVMRP (ang. Distance Vector Multicast Routing Protocol) - protokół routingu grupowego na podstawie wektorów odległości. Protokół ten opisano w dokumencie RFC 1075.

Protokół IPv6

Protokół IPv4 jest w dalszym ciągu powszechnie wykorzystywany pomimo niedoskonałości tego rozwiązania. Prace nad nowszą wersją protokołu IPv6 trwają od kilku lat. Jednym z ważniejszych argumentów przemawiających za potrzebą migracji do nowszej wersji protokołu jest zapotrzebowanie na dużą liczbę adresów Internetowych. Mechanizmy, o których będzie mowa w module poświęconym adresacji, wymyślone w celu efektywnego gospodarowania dostępną pulą IPv4 były dobre przy założeniu, że sieć komputerowa składała się tylko z typowych hostów i serwerów. Przy obecnych założeniach, że większość nowo dostępnych urządzeń powszechnego użytku będzie miało funkcje komunikacji sieciowej liczba tych adresów jest niewystarczająca. Innym powiązanym z poprzednim, wymaganiem jest potrzeba zapewnienia ustalonych parametrów transmisji dla ruchu multimedialnego. Technologie wprowadzane coraz powszechniej: telefonia IP, telewizja cyfrowa, wideo na życzenie itp. wymagają stałych parametrów przesyłania.

Innym, równie istotnym, wymogiem jest kwestia autoryzacji nadawcy, która nie była możliwa w IPv4.
Te oraz inne niewymienione czynniki bardzo istotnie przemawiają za szybką migracją do IPv6, który również bywa nazywany protokołem następnej generacji IPNG (IP Next Genaration).

Warto podkreślić fakt, że zmiana protokołu warstwy sieciowej modelu ISO (protokołu warstwy Internetowej stosu protokołów TCP/IP) nie powoduje potrzeby dostosowywania protokołów pozostałych. Część z dostawców Internetu (ISP) oferuje już dostęp do IPv6. Ze względu na fakt, że w dalszym ciągu powszechnie używany jest IPv4, to ruch IPv6 jest tunelowany w starszej wersji protokołu (IPv6-in-IPv4). Protokół IPv6 opisują dokumenty RFC 1883 oraz RFC 1884.

Jedną z podstawowych zalet, chociaż nie najważniejszą, jest liczba dostępnych adresów w nowej wersji protokołu. Ze względu na to, że do zapisania adresu w IPv6 użytych jest 128 bitów, to dostępna pula wynosi ok. 3,4x10^38 adresów. W przeliczeniu na powierzchnię Ziemi daje to ok. 6,7x10^17/mm^2. W ten sposób zapotrzebowanie na pulę adresów dla nowych rozwiązań sieciowych powinno zostać spełnione. Więcej informacji na temat adresacji znajduje się w dedykowanym module.

IPv6: budowa datagramu

Budowa datagramu IPv6 została przedstawiona na rysunku. Znaczenie pól jest zgodne z ich opisem:
Wersja - 4b - wersja protokołu IP, w tym przypadku 6
Priorytet / Typ ruchu (ang.Traffic Class) - 8b - pole służące do określenia priorytetu przesyłanego pakietu. Jest to szczególnie istotne w przypadku pakietów transmitujących ruch multimedialny, gdzie ważnym aspektem jest

zapewnienie wysokiego poziomu obsługi (ang. Quality of service). Pole to jest odpowiednikiem pola Type of Service w IPv4.
Etykieta przepływu (ang. Flow Label) - 20b - pole to zostało zarezerwowane na potrzeby zapewnienia wysokiego poziomu obsługi. Pole to składa się z kilku podpól: pierwsze cztery bity określają wrażliwość na zmiany czasów opóźnień, bity od 8 do 15 wyznaczają priorytet, reszta bitów identyfikuje potok danych.
Długość danych (ang. Payload length) - 16b - długość pola danych wyrażona wielokrotnością oktetów.
Następny nagłówek (ang. Next Header) - 8b - pole z informacją jaki będzie nagłówek rozszerzający. Ważną cechą tego pola, która umożliwia szybsze przesyłanie pakietów przez routery jest możliwość dołączania nagłówków rozszerzających. Szczegóły tego rozwiązania zostaną przedstawione na następnym slajdzie.
Limit przeskoków (ang. Hop Limit) - 8b - Liczba przeskoków, czyli liczba routerów, przez które pakiet może być przesłany zanim dotrze do celu. Po każdym przejściu przez router wartość tego pola jest zmniejszana o 1. Po osiągnięciu wartości 0 pakiet taki jest odrzucany. Odpowiednie pole w nagłówku IPv4 miało nazwę TTL. Maksymalna wartość tego pola podobnie jak pola TTL wynosi 255.
Adres źródłowy (ang. Source Address) - 128b - adres źródłowy
Adres docelowy (ang. Destination Addres) - 128b - adres docelowy

IPv6: nagłówki rozszerzające

Ważną cechą, która umożliwia szybsze przesyłanie pakietów przez routery jest możliwość dołączania nagłówków rozszerzających. Jest to możliwe, dzięki polu „Następny nagłówek” (ang. Next header). Nagłówek ten jest umieszczany w pakiecie za nagłówkiem podstawowym, a przed nagłówkiem warstwy transportowej. Nagłówki te powinny występować w określonej kolejności natomiast nie ma ograniczenia co do ich liczby. Nagłówki te zastępują pola opcjonalne w IPv4. Dzięki zastosowaniu tego mechanizmu możliwe jest, m.in. uwierzytelnianie pakietów. Dołączanie dodatkowych nagłówków pozwala na rozbudowywanie możliwości IPv6 bez potrzeby zmieniania formatu nagłówka głównego. Dołączenie nowego nagłówka jest sygnalizowane poprzez wpisanie liczby Next Header Value (NHV) w pole „Następny nagłówek”. Dodatkowo każdy z nagłówków rozszerzonych posiada również pole Next Header Value (NHV) przeznaczone na informację o ewentualnym następnym nagłówku.W ostatnim z nagłówków w polu Next Header Value (NHV) znajduje się wartość nagłówka określająca typ protokołu warstwy transportowej.
Wśród zdefiniowanych nagłówków dodatkowych można wymienić: Hop-by-hop options header Destinations options header-1 Source routing header Fragmentation header Authentication header IPv6 encryption header Destination option header-2

Podsumowanie

W module tym zostały przedstawione podstawowe protokoły warstwy Internetowej stosu protokołów TCP/IP. Protokół IP w wersjach 4 i 6 odpowiedzialny jest za dostarczenie pakietów do miejsca przeznaczenia. Ze względu na brak wbudowanych mechanizmów kontroli poprawności przesyłanych datagramów protokół IP posiłkuje się protokołem ICMP. Protokół IGMP wykorzystuje zalety rozsyłania grupowego do efektywnego przesyłania pakietów.

Dyrektor Domu Pomocy Społecznej
Ewa Orłowska