যেভাবে বাড়াবেন ওয়াইফাই নেটওয়ার্কের নিরাপত্তা

কে এম আলী রেজা

ওয়্যারলেস নেটওয়ার্কের ব্যবহার দিন দিন বাড়ছে। তাই হোম বা অফিস যেকোনো পর্যায়ে ওয়্যারলেস নেটওয়ার্কের সর্বোচ্চ নিরাপত্তা নিশ্চিত করা প্রয়োজন। এ লেখায় ওয়্যারলেস নেটওয়ার্কে আড়িপাতা ও ভাইরাস আক্রমণ প্রতিরোধসহ আরও কিছু আনুষঙ্গিক নিরাপত্তা সম্পর্কিত বিষয়ে আলোচনা করা হয়েছে।

আমরা অনেক সময় মনে করি, ওয়্যারলেস ল্যান বা নেটওয়ার্কের অ্যানক্রিপশন ফিচার চালু করলেই নেটওয়ার্কের নিরাপত্তা নিশ্চিত হয়ে যায়। কিন্তু উন্নত প্রযুক্তি জ্ঞানসম্পন্ন ওয়াইফাই হ্যাকারেরা এ ধরনের ব্যবস্থা ভেঙে ওয়্যারলেস নেটওয়ার্কে অনুপ্রবেশ করতে পারে এবং নেটওয়ার্ক ব্যবস্থায় বিভিন্ন ধরনের অনিষ্ট সাধন করতে পারে।

নেটওয়ার্কের ফিজিক্যাল নিরাপত্তা

ওয়্যারলেস নেটওয়ার্কের ফিজিক্যাল নিরাপত্তা একটি গুরুত্বপূর্ণ বিষয়, যদিও আমরা এ বিষয়টিকে অনেক সময় যথাযথ গুরুত্বের সাথে বিবেচনা করি না। আমাদের অসাবধানতার কারণে জ্ঞাতসারে বা অজ্ঞাতসারে নেটওয়ার্কের অনুমোদিত ইউজার বা বাইরের ইউজারের মাধ্যমে ওয়াইফাই ডিভাইস এবং নেটওয়ার্ক হার্ডওয়্যারের অপব্যবহার হতে পারে। যেমন, আমরা যদি নেটওয়ার্ক জ্যাক অসাবধানবশত খোলা রাখি, তাহলে যেকোনো ইউজার তার নিজস্ব অ্যাক্সেস পয়েন্টের (এপি) সাথে জ্যাকটি সংযুক্ত করে তার নিজস্ব ওয়্যাইফাই নেটওয়ার্কের শক্তি বাড়াতে পারে। এ ইউজার হয়তো অ্যাক্সেস পয়েন্টকে বহিরাগতদের অনুপ্রবেশ নিবৃত্ত করতে তথা নেটওয়ার্ক সিকিউরিটি দিতে যথাযথ ব্যবস্থা নেবে না। এছাড়া কেউ হয়তো উদ্দেশ্যপ্রণোদিতভাবে অ্যাক্সেস পয়েন্ট বা রাউটারকে ফ্যাক্টরি ডিফল্ট সেটিংয়ে রিসেট করে দিতে পারে। এর ফলে ওয়াইফাইয়ের সিকিউরিটি সেটিংগুলো অকার্যকর হয়ে যাবে। এ অবস্থায় ওয়াইফাই সীমার মধ্যে অননুমোদিত ইউজারেরা নেটওয়ার্কে অ্যাক্সেস পেয়ে যাবে।

ওয়্যারলেস নেটওয়ার্কের ফিজিক্যাল উপাদানগুলোর সুরক্ষার জন্য এগুলোকে এমন জায়গার স্থাপন করা প্রয়োজন, যাতে তা সাধারণ ইউজার ও বহিরাগতদের নজরে না আসে। নেটওয়ার্ক বিশেষ করে ইথারনেট ক্যাবল দেয়ালের ভেতর দিয়ে টানা প্রয়োজন। ক্ষেত্রবিশেষে ক্যাবলগুলো কোনো মোড়কের (কনডুইট) ভেতরে স্থাপন করা যেতে পারে। ইথারনেট জ্যাক নিরাপদ জায়গায় স্থাপন করতে পারেন, যাতে এগুলোর অ্যাক্সেস কেউ না পায়। নেটওয়ার্ককের অপ্রয়োজনীয়

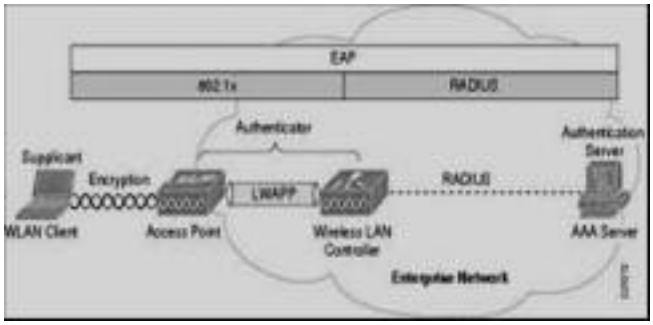
চিত্র-১ : সময়ভিত্তিক ১ এমবিপিএস ব্যান্ডউইডথ সেট করা

জ্যাকগুলো নিষ্ক্রিয় করে দিতে হবে।

802.1G· অথেনটিকেশনসহ এন্টারপ্রাইজ সিকিউরিটি ব্যবহার

অনেকেই জানেন, ওয়্যারলেস নেটওয়ার্কের WEP (Wired Equivalent Privacy) সিকিউরিটি ব্যবস্থা সহজেই ভেঙে ফেলা যায় এবং এর ভেতর দিয়ে অননুমোদিত ইউজারেরা নেটওয়ার্কে অ্যাক্সেস নিতে পারে। এ কারণে ওয়্যারলেস নেটওয়ার্কে WPA এবং WPA2 (Wi-Fi Protected Access) ব্যবস্থা ব্যবহার করা হয় পর্যাপ্ত সুরক্ষা পাওয়ার জন্য। তবে এ সুরক্ষা ব্যবস্থা ব্যবহারের দুটো ভিন্ন পদ্ধতি রয়েছে। এর মধ্যে একটি পার্সোনাল মোড, যার সেটআপ ও ব্যবহার খুব সহজ। তবে করপোরেট বা বিজনেস নেটওয়ার্কের ক্ষেত্রে এ মোডটি ব্যবহার না করাই ভালো। বৃহৎ এবং স্পর্শকাতর নেটওয়ার্কের ক্ষেত্রে একটি স্ট্যাটিক পাসফ্রেজ তৈরি করে তা এন্ড-ইউজার ডিভাইসে সংরক্ষণ করা হয়। এ পদ্ধতি এন্টারপ্রাইজ মোড হিসেবে পরিচিত। যদি কোনো ইউজার প্রতিষ্ঠান ছেড়ে যায় বা এন্ড-ইউজার ডিভাইস চুরি হয়ে যায়, তাহলে সে ক্ষেত্রে সব অ্যাক্সেস পয়েন্ট এবং এন্ড-ইউজার ডিভাইসে পাসফ্রেজ পরিবর্তন করতে হয়।

তুলনামূলকভাবে এন্টারপ্রাইজ মোড সেটআপ প্রক্রিয়া জটিল এবং এজন্য RADIUS (Remote Authentication Dial-In User Service) অথেনটিকেশন সার্ভার বা সার্ভিসের প্রয়োজন হয়। তবে এটি নেটওয়ার্কের সর্বোত্তম নিরাপত্তা নিশ্চিত করে। এ পদ্ধতিতে প্রত্যেক ইউজারের জন্য ইউনিক লগইন ক্রেডেনশিয়াল (ইউজার নেম ও পাসওয়ার্ড) নির্দিষ্ট করে দেয়া হয় এবং তা প্রয়োজনে সহজেই পরিবর্তন করা যায় বা প্রত্যাহার করে নেয়া হয়। কোনো ইউজার কোম্পানি ত্যাগ করলে বা ওয়্যারলেস ডিভাইস হাতছাড়া হয়ে গেলে তার জন্য নির্ধারিত লগইন ক্রেডেনশিয়াল প্রত্যাহার করা হয়। এতে একজন ইউজার অন্য ইউজারের ডাটা ট্রাফিক সম্পর্কে কোনো তথ্য জানতে পারে না, যা পার্সোনাল মোডে সম্ভব হয়।



চিত্র-২ : নেটওয়ার্ক সুরক্ষায় রেডিয়াস সার্ভার ব্যবহার

802.1G· ক্লায়েন্ট সেটিংয়ের নিরাপত্তা বিধান

WPA বা WPA2 নিরাপত্তা সিস্টেমে এন্টারপ্রাইজ মোড অধিকতর মজবুত। তারপরও এতে কিছু নিরাপত্তা ঘাটতি রয়েছে। যেমন, ইউজারের লগইন নাম ও পাসওয়ার্ড বাইরের কেউ জেনে যেতে পারে। অনেক সময় এগুলো হ্যাকিংয়ের শিকার হতে পারে। তবে এন্ড-ইউজার ডিভাইসে ক্লায়েন্ট সেটিংয়ের মাধ্যমে লগইন ক্রেডেনশিয়াল ডাটাবেজে বাইরের আক্রমণ প্রতিহত করা যায়। ক্লায়েন্ট পিসিতে এবং একে সাপোর্ট করে এমন সব ডিভাইসে নিশ্চিত করতে হবে, যেনো সার্ভার ভেলিডেশন ফিচারটি সক্রিয় থাকে।

নেটওয়ার্ক ঝুঁকি ও স্পর্শকাতরতা সম্পর্কে ইউজারদের সচেতন করা

নেটওয়ার্ক সুরক্ষা রাখতে নেটওয়ার্ক অ্যাডমিনিস্ট্রেটর হিসেবে আপনার অনেক দায়িত্ব থাকে। একই সাথে সাধারণ ইউজারেরাও সুরক্ষাকাজে অনেক গুরুত্বপূর্ণ অবদান রাখতে পারে। সাধারণ ইউজারদের সুরক্ষার বিষয়ে প্রশিক্ষিত করা এবং নেটওয়ার্ক ব্যবহারের বিষয়ে একটি কার্যকর নীতিমালা প্রণয়নের মাধ্যমে আপনি একটি ওয়্যারলেস নেটওয়ার্ককে নিরাপদ রাখতে পারেন। নেটওয়ার্ক অ্যাডমিনিস্ট্রেটর ইউজারদের পরামর্শ দিতে পারে তারা যেন নেটওয়ার্ককে কোনো ডিভাইস সংযুক্ত করা বা বিচ্ছিন্ন করার আগে অ্যাডমিনিস্ট্রেটরের

(বাকি অংশ ৬৪ পৃষ্ঠায়)